NUREG/CR-6636
BNL-NUREG-52566

Maintainability of Digital Systems: Technical Basis and Human Factors Review Guidance

Prepared by
William F. Stubler and James C. Higgins / BNL
Joel Kramer / NRC

Brookhaven National Laboratory

Prepared for
U.S. Nuclear Regulatory Commission

NUREG/CR-6636
BNL-NUREG-52566

Maintainability of Digital Systems: Technical Basis and Human Factors Review Guidance

Manuscript Completed:
Date Published:

Prepared by
William F. Stubler and James C. Higgins / BNL
Joel Kramer / NRC

Human Factors and Performance Analysis Group
Brookhaven National Laboratory
Upton, NY 11973

Prepared for
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
NRC JCN J-6012

ABSTRACT

There is currently a trend in nuclear power plants (NPPs) toward introducing digital technology into safety and non-safety systems. However, this equipment has characteristics different from older analog equipment and is susceptible to additional failure modes. Inadequate integration of digital systems into operating and maintenance practices, and inadequate understanding of the intricacies of software-based digital systems on the part of technicians and operators, can result in failures that render systems inoperable. Digital systems impose new demands on personnel for the testing, troubleshooting, servicing, and repair of hardware and software. This may become increasingly important as licensees, using the on-line maintenance capabilities of digital systems, perform more maintenance while the plant is at-power. The objective of this study was to establish human factors review guidance for the maintainability of digital systems based on a technically valid methodology. To support this objective, a characterization was developed for describing design features and practices important to maintaining digital systems. Then, technical information related to human performance in maintenance was reviewed. Information was drawn from nuclear power, process control, and aerospace domains and included reviews of maintenance practices and digital system failures. This information provided the technical basis on which guidelines were developed for reviewing design features that support maintenance. For some aspects the technical basis was insufficient to develop guidance; these were identified as issues to be addressed in future research.

CONTENTS

CONTENTS (Continued)

CONTENTS (Continued)

PART 2: Guidance for Maintainability Review

CONTENTS (Continued)

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

The Human-System Interface Design Review Guideline, NUREG-0700, Rev. 1, was developed to provide guidance on human factors engineering (HFE) to the U.S. Nuclear Regulatory Commission (NRC). The NRC staff uses NUREG-0700 for (1) reviewing the submittals of human-system interface (HSI) designs prepared by licensees or applicants for a license or design certification of a commercial nuclear power plant (NPP), and (2) conducting reviews of HSIs that could be undertaken as part of an inspection or other type of regulatory review involving HSI design or incidents involving operator performance. It describes those aspects of the HSI design review that are important to identifying and resolving human engineering discrepancies that could adversely affect plant safety. NUREG-0700 also details HFE guidelines for assessing implementations of HSI design.

In developing NUREG-0700, Rev. 1, several topics were identified as "gaps," because there was an insufficient technical basis upon which to develop guidance. One such topic is the integration of advanced HSI technology into conventional NPPs. The NRC is currently sponsoring research at Brookhaven National Laboratory (BNL) to (1) better define the effects of changes to HSIs brought about by applying digital technology on personnel performance and plant safety, and (2) develop guidance on HFE to support safety reviews if a review of plant modifications or HSIs is necessary. This guidance will be integrated into NUREG-0700 and will be used to provide the NRC staff with the technical basis to ensure that the modifications or HSI designs do not compromise safety.

The results of this project will contribute to satisfying the NRC's goals of (1) maintaining safety, (2) increasing public confidence, (3) increasing regulatory efficiency and effectiveness, and (4) reducing unnecessary burden.

Based upon literature, interviews, and site visits, the maintainability of digital systems was identified as an important human performance topic having potential safety significance. There is a trend in nuclear power plants (NPPs) toward introducing digital technology into safety and non-safety systems. There are many reasons for this, including the need to replace old equipment due to the high costs of maintaining it or the lack of support from vendors, and also the desire to enhance instrumentation and control (I&C) capabilities, the plant's performance, and reliability. Almost all analog systems in a NPP can be replaced with digital ones. These replacements may be of individual subsystems and components, or of entire systems.

Digital equipment has characteristics that differ from older analog equipment. Digital equipment is susceptible to different types of faults, the fault initiators may be different, and these faults may have different effects on plant performance. Reviews of digital systems found that software errors and inadvertent actions by personnel, particularly during maintenance, were leading causes of failures. Recent failures of digital systems in U.S. NPPs illustrate how the inadequate integration of digital systems into operating and maintenance practices, and inadequate understanding of the intricacies of software-based digital systems on the part of technicians and operators, caused them to become inoperable. The events also show that digital systems are susceptible to different failure modes than analog systems. These characteristics impose new demands on maintenance personnel for testing, troubleshooting, servicing, and repairing hardware and software. Maintainers must understand the characteristics of digital equipment, which may be more complex than older technologies; some skills learned for maintaining older equipment may be inadequate or inappropriate for digital equipment. Thus, while the human performance considerations associated with maintaining conventional equipment are relatively well understood, those associated with maintaining digital equipment are less clear.

The objective of this study was to develop HFE guidance, based on a valid methodology, to support reviews of maintainability aspects of digital system upgrades for existing plants. Our focus was HSI design. We recognize that other topics, such as software development and personnel selection and training, are important to maintaining digital systems. However, they are outside the scope of the current development effort and are being addressed by other NRC research projects. The objective was addressed through the following tasks:

- Development of a framework for characterizing aspects of digital systems, test equipment, maintenance procedures, and training aids important to maintenance

- Development of a technical basis for this topic using information sources that are highly valid, such as existing human factors standards, industry experience, and research on human performance

- Development of HFE review guidance for evaluating design features that support the maintainability of digital systems, following a format consistent with NUREG-0700, Rev. 1

- Identification of human performance considerations important to maintaining digital systems for which additional research is needed to develop NRC review guidance

The status of each will be briefly addressed below.

Characterization Framework

Existing systems were reviewed to identify the dimensions and characteristics along which the maintainability aspects of digital systems can be defined. Characterization was important because it provided a structure within which the reviewer could request information about a system, and with which to structure the guidance. The characterization was organized into the following four dimensions:

- Digital systems characteristics important to maintenance

- Testing and troubleshooting equipment
  - manual versus automatic test equipment
  - portable test equipment
  - built-in test equipment
  - display formats of test equipment
  - advanced troubleshooting aids

- Maintenance procedures

- Training aids

Technical Basis Development

Many sources of information were examined during this guidance development effort. Documents included existing human factors standards and guidelines, handbooks, and reviews of industrial incidents and maintenance practices. Additional information was obtained by visiting sites that used digital systems, and by interviewing subject matter experts from multiple domains either in-person or via telephone.

Based on our review, we concluded that the unique characteristics of digital systems can pose significant maintenance challenges. Computer-based processors, the key features of digital systems, add a degree of complexity that may not have existed in earlier I&C systems. Many interconnections can exist between digital components, subsystems, and systems, so that a single fault may affect many parts of a digital system. In some cases, the failure of a seemingly insignificant device, such as a ribbon on a peripheral printer, can start a cascade of failures that affect overall system performance. Also, the automatic capabilities of digital systems can change the system's configuration without direct input from personnel. For example, digital systems can automatically switch control capabilities between redundant processors but give little indication to maintenance personnel. Also, because software is a key component of digital systems, digital systems are highly susceptible to failures from software-related problems, such as its incorrect installation. In some cases, the effects of software-related problems are immediately apparent, such as when they actuate a safety system. In other cases, the effects may not be immediately apparent and may result in inoperable or improperly operating systems that provide few indications of their

condition. Another result may be undesirable system behavior that is triggered when a particular combination of conditions occurs.

With these characteristics, digital systems may be more susceptible to mistakes and slips during maintenance than conventional analog equipment. Mistakes can result from incorrect assessments of situations due to the subtlety of some operating and failure modes of digital systems. Thus, plant personnel may fail to notice automatic transfers of control between redundant processors. Such errors during maintenance have resulted in safety system actuations. Mistakes can also result if maintenance is inadequately planned. This may occur when maintenance and operations personnel fail to fully consider the unique characteristics of digital systems. Because of the complex relationships between components, subsystems, and systems, maintenance work can produce unexpected interactions within them. Predicting these interactions can be very demanding, so a formal analysis should be undertaken before conducting maintenance. Additional, informal analyses of conditions and effects may be required when troubleshooting, removing, replacing, and restarting (rebooting) equipment. Contributing factors may include inadequate or incomplete maintenance procedures and technical information from vendors.

The unique characteristics of digital systems can make them highly susceptible to failures from improperly executed but correctly planned actions (slips). Some slips include failure to follow steps properly (e.g., when rebooting a processor during on-line maintenance), mode errors (e.g., failure to recognize the current system mode), keying errors, and connection errors (e.g., connecting test equipment to the wrong port or wrong system). Some of these slips may reflect the poor transfer of maintenance skills learned on older equipment. For example, rebooting digital equipment may be quite different from restarting comparable analog equipment.

Troubleshooting is one area of maintenance that has been extensively studied in human factors research. Isolating a fault to a particular component within a digital system can impose high cognitive demands, requiring an extensive knowledge of the digital system and a great degree of troubleshooting skill. Demands on long-term memory, including recalling heuristics, testing practices, and unique characteristics of the equipment, may be quite high and may result in errors. In addition, the need to remember symptoms and organize test hypotheses can impose high demands on short-term and working memory. However, the human performance concerns associated with troubleshooting digital equipment appear to have more of an economic effect than a safety one for the nuclear industry. Because digital equipment is modular, malfunctions can be readily corrected by replacing circuit boards and other parts until the failure is found. Thus, the affected system can be rapidly restored to proper operation, and the task of troubleshooting the removed piece of equipment can be performed later.

Troubleshooting can place high demands on the maintenance organizations of NPPs. Many resources, including personnel, test equipment, materials, and time, may be devoted to trying to identify faults in the components removed from plant systems. For many of them, the original test results indicating that the component is faulty cannot be duplicated. As a result, the fault may never be found. This represents a drain on human resources, which may indirectly affect plant safety. If resources are diverted to troubleshooting, then fewer resources may be available for properly maintaining other equipment in the plant. Thus, off-line troubleshooting may *indirectly* threaten plant safety. However, other concerns, such as preventing mistakes and slips, may challenge plant safety more directly.

The human factors considerations associated with digital systems can be addressed in many ways. Design-oriented solutions may be applied to the maintenance-system interfaces of digital equipment and test devices to reduce maintenance errors. Administrative solutions may be applied in selecting and training of maintenance personnel and developing maintenance procedures.

HFE Review Guidelines

Once the technical information was assembled, a draft set of guidelines was developed. In general, guidelines were only developed for those aspects of maintainability that, in our interpretation, are supported by the literature. Extensive use was made of existing standards and guidelines that have undergone peer review. The HFE design guidelines were developed in the standard format adopted in NUREG-0700, Rev. 1. They are organized in eight

sections addressing the following topics: general considerations, instrument cabinets and racks, equipment packaging, fuses and circuit breakers, labeling and marking, adjustment controls, test points and service points, and test equipment.

Some of these topics support maintenance personnel in understanding the arrangement and status of components in digital systems; this guidance may reduce the likelihood of mistakes. For example, the topic, packaging of internal components, provides guidance for organizing digital equipment into individual modules to support maintenance personnel in searching for and isolating malfunctions. The topic, adjustment controls, provides guidance to ensure that maintenance personnel have adequate feedback when adjusting plant equipment. The topics, failure detection and isolation and test equipment, consider the presentation of test information to support personnel in detecting faults. Some topics represent good design practices that may reduce the likelihood of inadvertent actions (slips). For example, the packaging topic contains guidelines for preventing modules from being installed incorrectly and preventing functionally different modules from being interchanged. The labeling and marking topic contains guidelines that ensure that test points, service points, and components are properly designated to reduce their likelihood of being incorrectly identified by the maintainer. In addition, many topics contain good design practices to improve the overall efficiency of maintenance. This can improve system availability by reducing the time required for surveillance tests, preventive maintenance, and corrective maintenance.

The guidance was peer reviewed and revised. The new guidance will be integrated into the existing guidance in NUREG-0700, Rev. 1.

Remaining Human Performance Issues

Where there was insufficient information for the technical basis upon which to develop valid design review guidance, an issue was defined. Two issue areas were identified: (1) policies, procedures, and practices for ensuring maintainability, and (2) specified design topics in digital technology. For the first, we propose further research to develop process-oriented guidance, in a format compatible with NUREG-0711. Guidance should be developed for the appropriate elements of NUREG-0711 to specifically address considerations related to the maintainability of digital systems. The following are some of the specific topics included: HFE program development, HSI design, training, procedures, the development of automated test equipment and maintenance aids, and verification and validation of maintenance.

For the second area, further research should address the development of supplemental human factors guidance on specific digital technologies. While the guidance presented in this document is based on principles applicable to a broad range of technologies, digital technology continues to evolve at a rapid rate. Hence, human factors considerations related to the features of digital systems that are not explicitly addressed in the guidance developed in this document may be encountered in the future. The following topics were identified as being particularly important to maintaining digital systems: features that support on-line maintenance, advanced features of test and diagnosis equipment, and features of circuit cards and data buses that are related to maintenance errors.

PREFACE

This report was prepared by Brookhaven National Laboratory for the Division of Systems Technology of the U. S. Nuclear Regulatory Commission (NRC) Office of Nuclear Regulatory Research. It is submitted as part of the requirements for the project, "Human Factors Topics Associated with Hybrid Human-System Interfaces" (NRC JCN J-6012), specifically as part of Task 3, "Develop Review Approaches." The NRC Project Manager is Joel Kramer and the BNL Principal Investigator is John O'Hara.

ACKNOWLEDGMENTS

The authors wish to express their sincere gratitude to our colleagues Lew Hanes; Mike Fineberg and his review team at the Crew Systems Ergonomics Information Analysis Center (CSERIAC); and Bill Ruland, Greg Galletti, Jim Bongarra, Clare Goodman, Jim Stewart, and Rich Correia of the U.S. NRC for their review of the report. These reviewers provided insightful comments and perspectives on the issues addressed in the report and their knowledge and understanding significantly contributed to the study.

We also wish to thank Barbara Roland, Mary Anne Corwin, and Avril Woodhead for their preparation and careful technical editing of the report.

ACRONYMS

ALWR	Advanced light water reactor
ATE	Automatic test equipment
ATWS	Anticipated transient without scram
BIT	Built-in test
BITE	Built-in test equipment
BNL	Brookhaven National Laboratory
CFS	Consistent fault set
CR	Control room
CRT	Cathode ray tube
DOT	U.S. Department of Transportation
EPRI	Electric Power Research Institute
FAA	U.S. Federal Aviation Administration
HFDG	Human Factors Design Guide
HFE	Human factors engineering
HSI	Human-system interface
I&C	Instrumentation and control
LSI	Large-scale integrated circuit
LER	Licensee event report
NASA	National Aeronautics and Space Administration
NPP	Nuclear power plant
NRC	Nuclear Regulatory Commission
PLC	Programmable logic controller
PRA	Probabilistic risk assessment
RAM	Random access memory
RF	Radio frequency
ROM	Read only memory
SOCBI	Simulation-oriented computer-based instruction
URD	Utility Requirements Document
VLSI	Very large-scale integrated circuit

PART 1:

Development and Technical Basis

1 INTRODUCTION

1.1 Background

The Human-System Interface Design Review Guideline, NUREG-0700, Rev. 1 (O'Hara, Brown, Stubler, Wachtel, and Persensky, 1996), was developed to provide guidance on human factors engineering (HFE) to the U.S. Nuclear Regulatory Commission (NRC). The NRC staff uses NUREG-0700 for (1) reviewing the submittals of human-system interface (HSI) designs prepared by licensees or applicants for a license or design certification of a commercial nuclear power plant (NPP), and (2) conducting reviews of HSIs that could be undertaken as part of an inspection or other type of regulatory review involving HSI design or incidents involving operator performance. It describes those aspects of the HSI design review that are important to identifying and resolving human engineering discrepancies that could adversely affect plant safety. NUREG-0700 also details HFE guidelines for assessing implementations of HSI design.

In developing NUREG-0700, Rev. 1, several topics were identified as "gaps," because there was an insufficient technical basis upon which to develop guidance (O'Hara, 1994; O'Hara, Brown, and Nasta, 1996). One such topic is the integration of advanced HSI technology into conventional NPPs. The NRC is currently sponsoring research at Brookhaven National Laboratory (BNL) to (1) better define the effects of changes to HSIs brought about by applying digital technology on personnel performance and plant safety, and (2) develop guidance on HFE to support safety reviews if a review of plant modifications or HSIs is necessary. This guidance will be integrated into NUREG-0700 and will be used to provide the NRC staff with the technical basis to ensure that the modifications or HSI designs do not compromise safety.

The results of this project will contribute to satisfying the NRC's goals of (1) maintaining safety, (2) increasing public confidence, (3) increasing regulatory efficiency and effectiveness, and (4) reducing unnecessary burden.

Based upon literature, interviews, and site visits, the maintainability of digital systems was identified as an important human performance topic (O'Hara, Stubler, and Higgins, 1996). There is a trend in nuclear power plants (NPPs) toward introducing digital technology into safety and non-safety systems. There are many reasons for this, including the need to replace old equipment due to the high costs of maintaining it or the lack of support from vendors, and also the desire to enhance instrumentation and control (I&C) capabilities, the plant's performance, and reliability. Almost all analog systems in a NPP can be replaced with digital ones. These replacements may be of individual subsystems and components, or of entire systems.

Digital equipment has characteristics that differ from older analog equipment. Digital equipment is susceptible to different types of faults, the fault initiators may be different, and these faults may have different effects on plant performance. Reviews of digital systems found that software errors and inadvertent actions by personnel, particularly during maintenance, were leading causes of failures. Recent failures of digital systems in U.S. NPPs illustrate how the inadequate integration of digital systems into operating and maintenance practices, and inadequate understanding of the intricacies of software-based digital systems on the part of technicians and operators, caused them to become inoperable. The events also show that digital systems are susceptible to different failure modes than analog systems. These characteristics impose new demands on maintenance personnel for testing, troubleshooting, servicing, and repairing hardware and software. Maintainers must understand the characteristics of digital equipment, which may be more complex than older technologies; some skills learned for maintaining older equipment may be inadequate or inappropriate for digital equipment. Thus, while the human performance considerations associated with maintaining conventional equipment are relatively well understood, those associated with maintaining digital equipment are less clear.

This report documents the guidance developed for the maintainability of digital systems.

1.2 Organization of the Report

This report is organized into two parts. Part 1 discusses the methodology and technical basis for developing the guidance and contains the following sections:

Section 2, Objective, describes the overall objective of this research.

- Section 3, Methodology, describes the methodology used to develop the guidance.
- Section 4, Characterization of Digital Systems and Associated Maintenance Aids, identifies the characteristics of digital systems, test equipment, maintenance procedures, and training aids important to personnel performance and which should be addressed by HFE reviews.
- Section 5, Development of the Technical Basis, describes maintenance activities, including factors that may affect the ability of personnel to properly maintain digital systems.
- Section 6, Development of Guidance, describes the development of the review guidance.
- Section 7, Summary, is in two parts. The first summarizes the process of developing guidance, key human performance considerations, and the types of guidance developed. The second describes aspects of human performance that require further exploration before NRC review guidance can be established, and recommends ways to accomplish this.
- Section 8, References, provides references to documents cited in this report.

Part 2 contains Section 9, which has specific guidance for conducting safety reviews of human factors associated with the design characteristics of digital systems that affect personnel performance during maintenance tasks.

2 OBJECTIVE

The objective of this study was to develop HFE guidance, based on a valid methodology, to support reviews of the maintainability aspects of digital system upgrades for existing plants. Our focus was HSI design. We recognize that other topics, such as software development and personnel selection and training, are important to maintaining digital systems. However, they are outside the scope of the current development effort and are being addressed by other NRC research projects. The objective was addressed through the following tasks:

- Development of a framework for characterizing aspects of digital systems, test equipment, maintenance procedures, and training aids important to maintenance
- Development of a technical basis for this topic using information sources that are highly valid, such as existing human factors standards, industry experience, and research on human performance
- Development of HFE review guidance for evaluating design features that support the maintainability of digital systems, following a format consistent with NUREG-0700, Rev. 1
- Identification of human performance considerations important to maintaining digital systems for which additional research is needed to develop NRC review guidance

3 METHODOLOGY

3.1 Overview

Figure 3.1 shows the overall guidance development methodology for NUREG-0700. The process for developing the guidance is discussed in detail elsewhere (O'Hara, Brown, and Nasta, 1996; Stubler and O'Hara, 1996). The portion of the methodology applicable to this report and project is boxed in the figure. This section of the report describes the general rationale for developing the guidance.

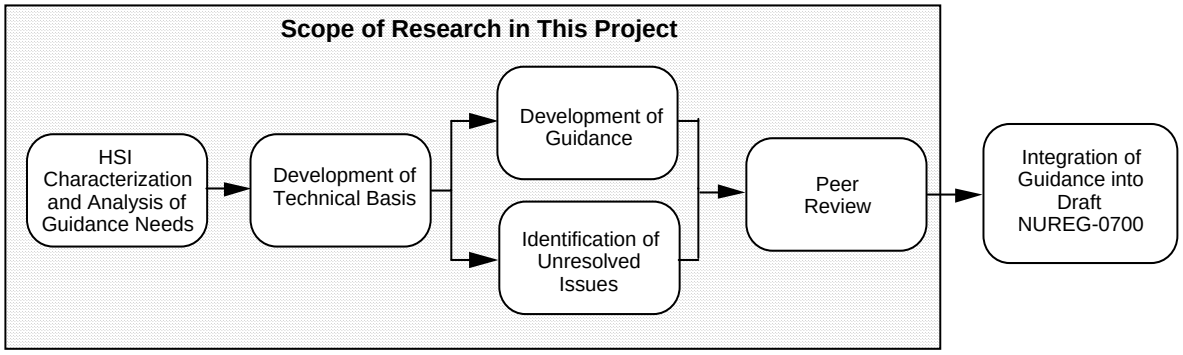

Figure 3.1 Major Steps in Developing NUREG-0700 Guidance

The methodology for guidance development was guided by the following objectives:

- Establishing a process that will result in valid, technically defensible, review criteria
- Establishing a generalizable process that can be applied to any aspect of HSI technology for which review guidance is needed
- Establishing a process that optimally uses available resources; i.e., developing a cost-effective methodology

The methodology places a high priority on establishing the validity of the guidelines. Validity is defined along two dimensions: internal and external validity. Internal validity is the degree to which the individual guidelines are based on an auditable technical basis. The technical basis is the information upon which the guideline is established and justified. The technical bases vary for individual guidelines. Some guidelines may be based on technical conclusions from a preponderance of empirical research evidence, some on a consensus of existing standards, while others are based on judgement that a guideline represents good practices based on the information reviewed. Maintaining an audit trail from each guideline to its technical basis serves several purposes by allowing

- the technical merit of the guideline to be evaluated by others
- a more informed application of the guideline since its basis is available to users
- deviations or exceptions to the guideline to be evaluated

External validity is the degree to which the guidelines are subjected to independent peer review. The peer review process is a good method of screening guidelines for conformance to accepted HFE practices and for comparing guidelines to the practical operational experience of HSIs in real systems.

For individual guidelines, these forms of validity can be inherited from the source documents that form their technical basis. Some HFE standards and guidance documents, for example, already have good internal and external validity. If validity is not inherited, however, it should be established as part of the guidance development process. The NUREG-0700 guidance development methodology was established to provide validity both inherited from its technical basis and through the guidance development and evaluation process.

Figure 3.2 depicts the process used to develop the technical basis and guidance. The process emphasizes information sources that have the highest degree of internal and external validity for the development of the technical basis. Thus, primary and secondary source documents were sought as sources of guidance first, followed by tertiary source documents, basic literature, industry experience, and other sources. From these information sources, design principles and lessons from industry experience were identified. Using this technical basis as a foundation, the guidance was developed. For specific aspects of the topic, in which there was an inadequate technical basis to develop guidance, unresolved research issues were defined. Thus, the analysis of information led to the development of both guidance and issues. The resulting guidance documentation includes HFE guidelines, technical basis, the development methodology, and unresolved research issues.

Each of the steps of this research activity – topic characterization, technical basis development, guidance development and documentation, issue identification, and peer review – is discussed in greater detail in the sections that follow.

3.2 Characterization of Maintenance

The first step in developing guidance was to identify the areas for which it was needed. Information on maintaining digital systems was reviewed to identify the characteristics of digital systems and related tasks that are relevant to reviews. Characterization provides a structure within which a reviewer can request information about a digital system or maintenance practices. It also is the structure used to organize the guidance for design review.

An initial characterization of this topic was given in an earlier BNL report (O'Hara, Stubler, and Higgins, 1996). It was expanded and refined based on information from the following sources:

- Reviews of failures of digital systems conducted by the NRC, foreign regulatory agencies, and independent researchers

- The technical bases of HSI and I&C requirements for advanced light water reactors (ALWR), presented in the Electric Power Research Institute's Utility Requirements Documents (EPRI URD) (EPRI, 1992, 1993)

- Reviews of maintenance practices for digital systems sponsored by the NRC, the Federal Aviation Administration (FAA), the U.S. Department of Transportation (DOT), and industry organizations

The characterization of digital systems and associated maintenance aids is given in Section 4.

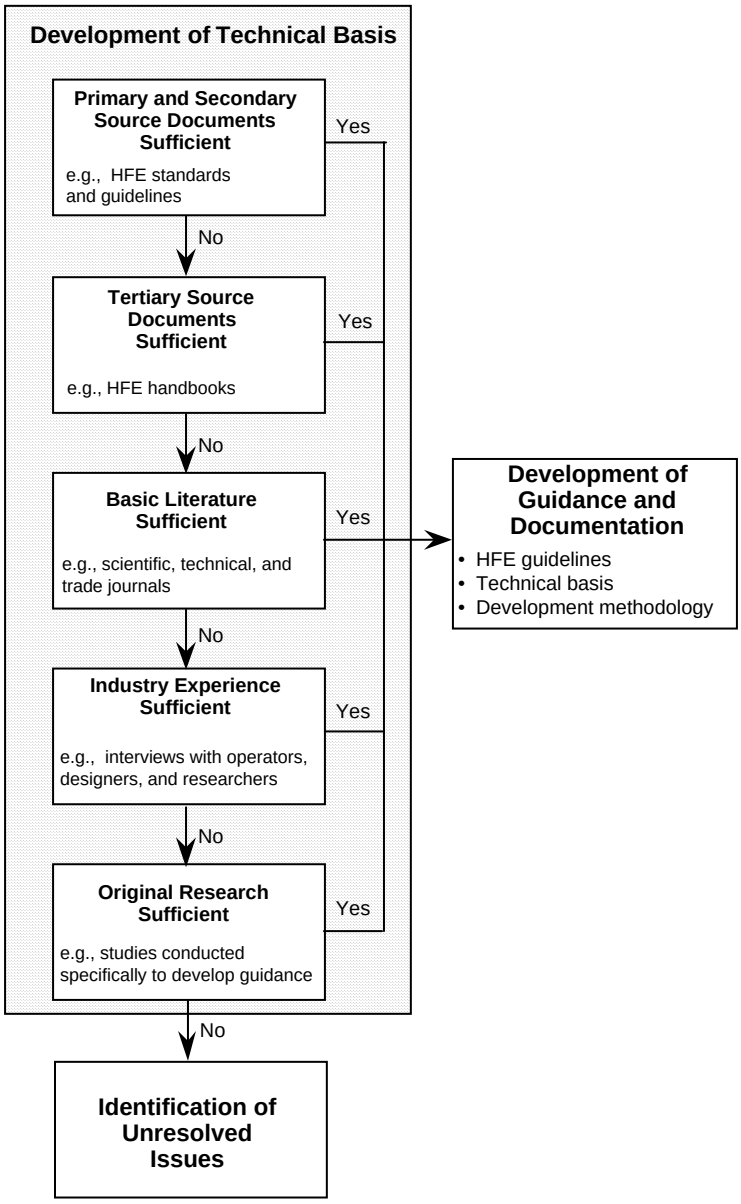

Figure 3.2 Technical Basis and Process for Developing Guidance

3.3 Development of Technical Basis

The development of detailed review guidelines for maintaining digital systems began by identifying, gathering, and reviewing the technical information upon which the guidance would be based (see Figure 3.2). The process was designed to develop valid guidance in the most cost-effective manner. First, primary source documents were sought. These were HFE standards and guidance documents possessing internal and external validity. That is, these documents generally had their own research bases, and their authors considered research and operational experience. Such documents may include human factors standards and guidelines that have an empirical basis and were found to be acceptable through peer review. Secondary sources included human factors guidelines and standards developed for complex, human-machine systems having either strong internal or external validity, but not both. Documents without internal and external validity were considered tertiary sources. Our preference was to use documents with established validity.

In addition, the findings from basic literature were analyzed (articles from technical journals, research organizations, and technical conferences). For this literature, engineering judgement was required to generalize from the unique aspects of individual studies to applications in the workplace. Individual experiments often had unique constraints that limited their generalizability (such as their unique participants, types of tasks performed, and types of equipment used). For example, most laboratory experiments do not involve tasks of the complexity of NPP operations, nor do most examine them under the same performance shaping factors (such as rotating shifts, stress, and fatigue) as exist in a work environment. While information from empirical research is a valuable part of guidance development, it usually cannot be blindly adopted, and must be interpreted and judged in the context of real-world tasks and systems, based on professional and operational experience.

Industry experience includes published case studies, surveys, and interviews with knowledgeable domain experts about incidents and accepted practices from a variety of industries. Although such information may lack a rigorous experimental basis (and thus, a measure of validity), it has high relevance.

The technical basis development methodology stopped at this point. Where additional issues are identified, it is possible to conduct original research. This approach has the advantage of being focused on specific issues of interest and has both high relevance and a sound experimental basis from which to establish validity. It is generally given the lowest priority because of the time and cost required to conduct original research.

The following describes two key information sources: the source documents, and site visits and interviews.

Source Documents

The review of human factors literature revealed a long history of documents devoted to the topic of maintenance, including primary, secondary, and tertiary documents. Literature from defense research considering general human factors in maintenance, such as job aiding, maintainability engineering, system design, and task analysis, dates from the 1950s and 1960s (Majoros and Boyle, 1997). This early guidance, which pre-dates the widespread use of digital technology, includes design principles that are broadly applicable to many technologies. Many of these earlier general themes and principles are reflected in later guidance documents.

Guidance on digital systems evolved in two ways in the 1980s and 1990s. First, by tailoring general principles from earlier, more general guidance, and second, by developing new guidance to address the special characteristics of digital technology. The following are important documents giving human factors guidance on maintaining digital equipment:

- Human Factors Design Guidelines for Maintainability of Department of Energy Nuclear Facilities, UCRL-15673 (Bongarra, Van Cott, Pain, Peterson, and Wallace, 1985)

- Human Engineering Design Guidelines For Maintainability, EPRI NP-4350 (Pack, Seminara, Shewbridge, and Gonzalez, 1985)
- Recommendations to the NRC on Human Engineering Guidelines for NPP Maintainability, NUREG/CR-3517 (Badalamente, Fecht, Blahnik, Eklund, and Hartley, 1986)
- Man-System Integration Standards, NASA-STD-3000 (NASA, 1987)
- Man-System Integration Standards, NASA-STD-3000B (NASA, 1995)
- Advanced Light Water Reactor Utility Requirements Document, Volume II, ALWR Evolutionary Plant, Chapter 10, Man-Machine Interface Systems, EPRI URD (EPRI, 1992)
- Advanced Light Water Reactor Utility Requirements Document, Volume III, ALWR Passive Plant, Chapter 10, Man-Machine Interface Systems, EPRI URD (EPRI, 1993)
- NRC Review of Electric Power Research Institute's Advanced Light Water Reactor Utility Requirements Document, Chapter 10 Man-Machine Interface Systems, NUREG-1242, Vol. 3, Part 2 (NRC, 1994)
- Human Factors Design Guide (HFDG): For Acquisition of Commercial Off-The Shelf Subsystems, Non-Developmental Items, and Developmental Systems, DOT/FAA/CT-96/1 (Wagner, Birt, Snyder, and Duncanson, 1996)
- Human Factors Guide for Aviation Maintenance, Version 2.0, GPO Document 050-007-01098-2 (Galaxy Scientific Corporation, 1996)

Bongarra et al. (1985) provided maintainability guidance for U.S. Department of Energy facilities, while Pack et al. (1985) gave industry-sponsored guidance for NPPs. Both documents were extensive, covering a broad range of topics, including some relevant to servicing electrical equipment. Badalamente et al. (1986) had the stated purpose of offering selected HFE guidelines to reduce the incidence of design-induced maintenance errors, and thereby increase the operational safety of NPPs. The guidelines were grouped in seven categories: accessibility and workspace, physical environment, loads and forces, maintenance facilities, maintenance tools and equipment, operating equipment design, and information needs. While the scope of this document also was broad, the guidance on electrical and electronic equipment was more limited than in the two earlier documents. The National Aeronautics and Space Administration (NASA) developed the Man-System Integration Standard (NASA, 1987) to provide guidance to support aerospace projects, such as Space Station Freedom. This document was revised and most recently issued as NASA (1995); it includes a chapter on maintainability. While much of this guidance was derived from earlier sources, it was tailored to the unique considerations of spacecraft. Thus, some care is warranted when applying this guidance to earth-bound facilities, such as NPPs.

The EPRI URDs (EPRI, 1992, 1993) were developed as part of an effort by the nuclear power industry to establish requirements for future advanced light water reactors. Chapter 10, Man-Machine Interface Systems, sets out the requirements for I&C systems. Volume II covers evolutionary plants and Volume III addresses passive plants. However, the guidance for maintaining I&C systems is essentially the same in both volumes. These documents are important because they explore the capabilities and limitations of current digital technologies. The NRC reviewed these documents in NUREG-1242, NRC Review of Electric Power Research Institute's Advanced Light Water Reactor Utility Requirements Document; the most recent version is NRC (1994).

The Human Factors Design Guide (Wagner et al., 1996) "...consolidates guidance from the source materials of several government agencies and provides one reference for application to new systems associated with the Federal Aviation Administration" (p. 1-1). This guide describes a broad range of human factors topics in addition to maintenance, and extensively tracks specific guidelines to their source documents.

3 METHODOLOGY

Of the ten documents described, we considered the first nine as primary source documents for this work. The human factors guideline documents (Bongarra et al., 1985; Pack et al., 1985; Badalamente et al., 1986; and Wagner et al., 1996) all contain guidelines that have clear technical bases, either in accepted practices or empirical research, and were peer reviewed. The EPRI URDs may be considered primary source documents because they present an industry consensus of acceptable practices. Human factors professionals participated in their development and they were favorably reviewed by the NRC. NUREG-1242 is a primary source document because it represents the NRC's position on the EPRI URD documents.

The Human Factors Guide for Aviation Maintenance, Version 2.0 (Galaxy Scientific Corporation, 1996) is an edited volume that compiles human factors principles and industry practices for aircraft maintenance. The individual chapters were written by highly regarded professionals. This document has a discussion format, rather than a guidelines format. Its primary emphasis is on maintenance processes, rather than on the design characteristics that support maintenance activities. Because this document does not explicitly track guidelines to source documents, it is difficult to distinguish guidance that has an extensively reviewed technical basis from that based on the authors' opinions. Therefore, we classified it as a tertiary source.

Since recent documents tend to include guidance from earlier documents, and usually update it, the decision was made to focus on the most current source documents. Thus, guidance was obtained first from DOT/FAA/CT-96/1 (Wagner et al., 1996) the EPRI URD (EPRI, 1993), and NUREG-1242. If the guidance from these documents was considered unclear, incomplete, or difficult to apply to digital systems in NPPs, then the source documents for the guidance were reviewed. For example, DOT/FAA/CT-96/1 cites UCRL-15673 as a source. If a particular guideline from DOT/FAA/CT-96/1 was difficult to apply to NPPs, the original guidance from UCRL-15673 may be cited instead. Section 8, References lists the full set of information sources used in preparing this document. Other guidance was based on practices of other industries that have extensive experience with maintaining digital systems. Lessons learned from them were used for developing guidance when they were consistent with sound HFE principles, such as the high-level HSI design review principles presented in Appendix A of NUREG-0700, Rev. 1.

Site Visits and Interviews

Additional information about industry practices and human factors challenges associated with the maintainability of digital systems was obtained by speaking with personnel from various industrial and research facilities. The following were contacted via either a site visit or telephone interview:

- One foreign NPP with computer-based HSIs and digital control systems (operators, trainers, and HSI design personnel)
- One domestic NPP upgraded with digital control systems (operators, maintenance, and design personnel)
- Two coal-fired power plants with computer-based HSIs (operators and HSI design personnel)
- Five chemical plants with computer-based HSIs (operators, supervisors, and HSI design personnel)
- NASA/Johnson Space Center (HFE project manager, formerly in charge of human factors requirements for an on-board maintenance workstation for Space Station Freedom)
- Federal Aviation Administration, Office of Aviation Medicine, Washington, DC (HFE program manager for aircraft maintenance)
- Federal Aviation Administration, William J. Hughes Technical Center, Atlantic City, NJ (HFE program manager for central maintenance of air traffic radar systems)

- Naval Air Warfare Center, Patuxent River, MD (a senior human factors engineer involved in the design and maintenance of cockpits for military aircraft)

- HFE consultant to the FAA for commercial aviation maintenance

The industry practices and human performance considerations identified through these interviews and site visits were incorporated into the technical discussion in Section 5, Human Performance Considerations Associated with Maintenance, and supported the selection and development of guidance topics.

3.4 Guidance Development and Documentation

Once the technical information was assembled, it was compared to the information needs established earlier and then information was extracted from the various source documents. The scope of this guidance development effort was restricted to maintenance topics that related to both human performance and digital systems. Topics that were considered to be related to human performance included design or task characteristics that (1) *could affect* personnel performance (e.g., cause errors), and (2) *could be affected by* personnel performance (e.g., are highly susceptible to human errors). A draft set of guidelines was compiled from the information in the technical basis. The guidelines were organized and specified in a standard format. (See Section 6 for a more detailed discussion of this process.) The guidelines themselves are presented in Part 2 (Section 9) of this document.

3.5 Identification of Issues

Where there was insufficient information to provide a technical basis for valid design review guidance, an issue was defined, as described in Section 5.5.

The issues reflect aspects of digital-system maintenance that require additional research. From a design review standpoint, the issues reflect aspects that will have to be addressed on a case-by-case basis, as for example, during design-specific tests and evaluations.

3.6 Peer Review

The technical basis and guidance was submitted for review by experts including personnel from the U.S. NRC with expertise in human factors engineering and related engineering fields. Human factors specialists who are external to the NRC and have expertise in human performance in complex systems, such as NPPs and aviation, also reviewed the guidelines. These external reviews included evaluations of the topic characterization with the following criteria: clarity, accuracy, and completeness. The technical basis was evaluated with its organization, necessity, sufficiency, resolution, and basis in mind. Comments from the peer reviews were incorporated into the present version of this document.

4 CHARACTERIZATION OF DIGITAL SYSTEMS AND ASSOCIATED MAINTENANCE AIDS

This section describes design characteristics that should be considered when reviewing upgrades involving digital systems, and includes descriptions of general design characteristics of digital systems, test equipment, and information aids that may affect personnel performance during maintenance. Digital systems introduced into NPPs as upgrades are likely to have some or all of these characteristics. In addition, much of the plant equipment may retain its original analog design. Thus, the resulting design will be a hybrid of digital and analog systems, subsystems, and components.

4.1 Digital Systems

Installing digital equipment in NPP systems may range from replacing individual subsystems and components to entire systems, for example, completely replacing an analog monitoring system with a system that is based entirely upon digital technology. As another example, a control system consisting of sensors, processors, controls, displays, and equipment actuators, may have its analog processors upgraded with digital processors, rather than replacing the entire system. However, when a digital processor is installed, it may be necessary to install additional signal converters to translate the analog signals into digital format and then translate the digital output of the processor back into analog format for the rest of the system.

One way to describe digital systems is to compare them to analog systems. Both analog and computer-based, digital systems can monitor, control, and protect critical plant equipment, safety systems, and processes. However, they perform these functions differently. Analog systems are composed of circuitry for processing analog signals (e.g., continuous signals that vary along a continuum). Digital systems consist of digital components, such as microprocessors, programmable logic controllers, and integrated circuit boards, which process digital (i.e., discrete) signals. Their functions are primarily defined by sets of instructions (software code), rather than by hardware components, and these instructions are executed via data processing and transmission equipment (hardware) (Lee, 1994). Some potential benefits of digital technology include the smaller size of components, lower power consumption, greater flexibility for modifications, greater stability of signals (e.g., less tendency to drift), and the potential for higher reliability. However, they are susceptible to computer software and hardware failures, which differ from the types of failures that occur in analog components (Klauer, Gravelle, Schopper, and Howell, 1993).

Failure rates related to operating analog components often are characterized by a "U-shaped" curve. The greatest number of failures tend to occur during the initial "burn-in" period when they are first put into service, and then toward the end of their serviceable life (Johansson, 1996). In addition, the performance of analog components tends to degrade slowly until they fail.

Digital systems may contain hardware with "U-shaped" failure patterns similar to analog systems. However, the software code of digital system software is prone to a different failure pattern. Software failures are typically due to design or programming errors that exist from the inception. If they are not detected and corrected during initial testing, these errors may remain hidden until the proper combination of conditions is present; failures typically occur when conditions trigger the execution of an incorrect set of instructions. Consequently, the software portions of programmable digital systems do not tend to have increased failure rates over time; that is, the software does not "wear-out" through use. "If a program is fault-free, it will remain fault-free forever, provided the environment in which the program operates does not change" (Johansson, 1996, p. 709).

In addition, digital components are susceptible to sudden failures and sudden recovery throughout their operating life (Wiener and Nagel, 1988). Failures may be due to many factors, including software errors and common-mode and common-cause failures of software and hardware. Sudden failures may reflect susceptibility of integrated circuits to electromagnetic interference due to their high operating frequencies and low voltages, and to physical faults. Like analog equipment, digital equipment may fail due to improper modifications or changes in controls. The actions of

operators or maintainers may cause failures through the improper entry of data or instructions for the computer, and improper handling of hardware components. Since thousands of circuits may reside on a single chip, the failure of a single integrated circuit may cause multiple components of a digital system to malfunction (Klauer et al., 1993).

A standard design approach for ensuring the reliability of plant systems is to have redundant channels for a particular function, each consisting of sensors, processors, and transmitters that perform the same function. If one channel fails, the other channel(s) ensures that the function is carried out properly. Another type of redundancy employed for both analog and digital safety systems is "within-channel" redundancy for selected components. A digital upgrade can have within-channel redundancy by providing multiple, redundant processors and other components. Thus, if the primary processor fails, one or more backup processors assume the proper operation of the channel. Control is transferred from the primary processor to a backup processor automatically, and is usually accompanied by an indication either locally or in the control room (CR). It may also be possible to effect transfer through a local manual action or one in the CR.

Control systems that feature redundant digital processors and fault-diagnostic routines are called fault-tolerant digital control systems because they can detect single faults and isolate the failed component(s) within the channel (Paula, Roberts, and Battle, 1993). The advantage of such systems is that they will continue to function after most single hardware faults (i.e., multiple faults must occur before they stop functioning). Control channels lacking this feature typically stop after a single fault. Fault-tolerant capabilities can enhance the reliability of a control system. They have been found to be more reliable than control channels that have no internal redundancy (e.g., no redundant processors), and often out-perform the reliability of analog control systems (Paula et al., 1993). Some variations of fault-tolerant, digital control systems include dual redundant systems (two redundant processors in a channel), triple-modular-redundant systems (three redundant processors in a channel), and triple-modular-redundant systems that reconfigure to dual redundancy after the first failure in the channel (Paula et al., 1993).

Digital systems featuring redundant processors often have a characteristic particularly significant to maintenance – they allow certain maintenance activities, such as changing software parameters, setpoints, and logic configurations, and resetting processors, to be performed while the plant is operating at power (NRC, 1996). Typically, control of the affected plant system is transferred to one processor while maintenance is performed on one or more of the redundant processors. On-line maintenance can increase the system’s and plant’s availability because systems do not have to be shut down for it. However, on-line maintenance can also increase the safety consequences of maintenance errors because the plant is operating while maintenance is being undertaken.

These digital systems have another characteristic important to maintenance. Before control can be transferred from one processor to another, their output signals must be matched. If they are not matched and a large difference exists between them, the system may receive a signal instructing it to make a large change over a short time. If the system cannot respond properly, a "bump" is said to occur. Some bumps can cause safety system actuations. In many control systems, the outputs of redundant processors are matched automatically. However, in some configurations, such as manual control and test modes, matching may not be automatic, and people may be required to take additional actions to ensure a smooth transfer.

Digital systems may be described in terms of progressively smaller units. Wagner et al. (1996) define a unit of equipment as an assemblage of items that may include modules, components, and parts that are packaged together into a single hardware package. They define a module as an assemblage of two or more interconnected parts or components comprising a single physical entity with a specific function. A module may be a printed circuit board or a smaller unit containing individual components that plugs into a printed circuit board. A component is defined as a subdivision of a unit of equipment that can be treated as an object by the maintainer, but which can be further separated into parts; a mounting board together with its mounted parts is an example. A part is an object that cannot be broken down further without destroying its designated use, such as fuses, circuit breakers, transistors, resistors, capacitors, and integrated circuit chips.

4 CHARACTERIZATION OF DIGITAL SYSTEMS

A chip, such as a large-scale integrated circuit (LSI) or a very large-scale integrated circuit (VLSI) may contain thousands of logic gates, shift registers, counters, read only memory (ROM) and random access memory (RAM) microprocessors, and microprocessor-support circuits (Klauer et al., 1993). Such integrated circuits are very compact compared to analog circuits that supply similar functions, and have advantageous electrical properties, such as low power consumption, high information-transfer rates (bits per second), and low radio frequency (RF) emissions. Many chips may be installed on a single printed circuit board (Klauer et al., 1993).

Printed circuit boards are often installed in cabinets or other enclosures by being inserted into edge connectors. Dozens of physically similar printed circuit boards may be inserted side-by-side into the backplane of an enclosure to form a subsystem – a collection of electrical modules that perform a particular function (Klauer et al., 1993). A plant system, such as a digital feedwater control system, may be composed of multiple subsystems. These definitions are used throughout this document, including the guidelines in Section 9.

The unique characteristics of digital equipment can result in properties that affect the ways maintenance can be performed; some of them are described below.

Susceptibility to Physical Damage – Unlike many mechanical components in NPPs, digital components are often small, relatively fragile, and easily damaged by handling. Furthermore, characteristics of the maintenance work environment may increase the likelihood of such physical damage. One factor may be the accessibility of electrical cabinets and their contents, and the manual dexterity of maintenance personnel. Therefore, maintenance personnel must handle digital components carefully.

Susceptibility to Spurious Signals – Because of their high operating frequencies and low voltages, the integrated circuits of digital equipment are susceptible to faults caused by spurious signals originating from electromagnetic interference, static electricity charges, and sudden voltage changes. Personnel must take care when handling digital components or when working nearby to avoid exposing digital equipment to these sources; a static electric discharge from a maintenance worker may cause a spurious signal that disrupts the operation of a system.

Susceptibility to Software Errors – Software errors are instructions that exist in computer code that can cause a computer-based system to behave undesirably. Software errors are a form of latent error (Reason, 1990; Reason and Maddox, 1996) that can lie dormant indefinitely until a certain combination of conditions triggers them. For example, a software error may have no apparent effect on a digital system until a particular combination of factors (e.g., plant state, system state, and personnel actions) causes the instructions to be executed in a way that produces undesirable behavior in the digital system (Paula et al., 1993). Software verification and validation procedures (i.e., tests and analyses) provide a structured approach to look for and detect software errors created during the design process; this is addressed by other NRC guidance. Additional software errors may be introduced during maintenance. For example, if there are multiple versions of the software, personnel may install the wrong version (e.g., load the wrong computer file). Also, installing software sometimes requires the person to enter data (e.g., the date and time) or instructions (e.g., commands for loading and saving), and if they are not entered correctly and in the proper sequence, the software may not operate properly. Thus, personnel who maintain software must ensure that the correct versions are used, and that additional commands and data used during its maintenance are correct and in sequence.

Susceptibility to Complex Interactions with Other Equipment – Since a single chip may have thousands of circuits, the failure of a single-integrated circuit may cause multiple components of the digital system to fail (Klauer et al., 1993). Complex relationships may exist between subsystems and systems. Thus, an important characteristic of digital systems is the possibility of interactions between components, subsystems or systems going awry. For

example, Ragheb[1] reports that in one foreign NPP, a mechanical problem with the printing ribbon of a peripheral computer resulted in a reactor transient:

> Jamming of a computer printer ribbon caused its buffer to fill and stop the execution of a program. This caused the control computer to stall and close the cooling flow supply valves to the fuel tube. The event prompted recommendations for software and hardware changes to ensure cooling flow to the fuel is maintained at all times in cases of computer stalls (p. 6).

Further, maintenance can influence these interactions by affecting the operating status of equipment and the links between equipment; for example, by removing equipment from, or returning it to, service. Such interactions require careful analysis to identify and understand.

The characteristics of digital equipment may influence maintenance practices. For example, the complexity of software can complicate tests and troubleshooting, but the modularity of digital components makes these systems easier to disassemble. Compared to analog equipment, there may be a greater tendency to remove digital components suspected of being faulty, replace them immediately, and then take the suspect components elsewhere for testing and repair. Section 5 describes human performance considerations associated with changes in maintenance practices.

4.2 Testing and Troubleshooting Equipment

Test equipment is used by maintenance personnel to assess the status of systems and locate faults. Wagner et al. (1996) state that the purpose of test equipment is to simplify the job of the maintainer, reduce the preparation or turn-around time for installing, maintaining, and repairing systems, and reduce total maintenance costs. This equipment is used to support periodic surveillance tests, periodic maintenance, and unscheduled maintenance due to failures. Accordingly, test equipment should be fast, easy, and safe to use (Wagner et al., 1996).

With the introduction of digital upgrades in NPPs, traditional testing and troubleshooting tools and methods may not be adequate because of the complexity of the task. Maintenance personnel may face new tasks imposing cognitive and physical demands that differ from those of traditional testing and troubleshooting tasks. The following describes some design characteristics relevant to testing and troubleshooting for digital systems. These characteristics may be integral parts of the plant equipment, such as built-in test (BIT) capabilities, or separate pieces of maintenance equipment. During maintenance, personnel must interact with the user interfaces of both the plant's equipment and the separate test equipment.

4.2.1 Manual Versus Automatic Test Equipment

The degree of automation of test equipment can vary. Fully manual test equipment usually requires the maintainer to perform tests one at a time, as with a standard voltmeter. To use it, the maintainer places a pair of leads across two contact points on the equipment, reads the voltage, and compares this value to the range of acceptable or expected values. After completing the tests for one pair of test points, the maintainer proceeds to the next pair. By considering the voltage values for one or more sets of points, the maintainer determines whether the components connected to the test points are functioning properly.

---

[1]Ragheb, H. (1996). Operating and maintenance experience with computer-based systems in nuclear power plants. Presented at the International Workshop: Technical Support for Licensing of Computer-Based Systems Important to Safety, Munich, Germany. (Available form H. Ragheb, Directorate of Reactor Regulation, Atomic Energy Control Board, Ottawa, Canada, K1P5S9.)

Automatic test equipment (ATE) can check two or more signals in sequence without the intervention of a maintainer (Wagner et al., 1996). They are usually programmable devices designed to detect faults by exercising a set of functions of a particular portion of a digital system (Klauer et al., 1993). ATEs are intended to relieve some of the burdens of manually testing digital systems. The tests may be focused at a high level, such as the operation of a subsystem, or at a low level, such as on an individual component. Thousands of tests may be rapidly administered with minimal human intervention. For example, many integrated circuits, such as microprocessors, may require several hundred unique test patterns to verify that they are operating properly. ATE tests usually stop after the first out-of-tolerance signal is detected (Wagner et al., 1996).

An important consideration is how the tests are initiated; some categories are as follows:

- Continuous tests – Tests are run constantly and a message is generated when a failure is detected. This message may be an alert to plant personnel or an entry into a computer-based log.

- Automatic initiation – Tests may be initiated on a fixed schedule or when a particular event occurs.

- Manual initiation – Tests are initiated by plant personnel, and may include diagnostic tests that are only performed when the maintainer is interested in the status of equipment, or when periodic surveillance tests are required. ATEs may operate like manual test equipment by including stopping points in the test program. At these points the maintainer can decide whether the testing program should continue or whether certain tests should be repeated.

The appropriateness of these different types of initiation partly depends on the type of information needed. For example, if personnel need to know when a system fails, then continuous testing may be the best, because it detects failures sooner than periodic testing. Manual initiation may be appropriate when information is only needed under certain circumstances, as, for example, when a maintainer needs the results of a diagnostic test to locate the cause of a malfunction.

A major advantage of ATE is that it can make a rapid sequence of checks with little or no chance of omitting steps. Its disadvantages include the following (Bongarra et al., 1985):

- Cost, size, weight, and maintenance requirements are relatively high.

- The test equipment may be specialized, with limited versatility.

- Self-checking features are needed to detect test equipment malfunctions, adding to the cost and problems of maintaining the test equipment.

- The test equipment may require modifications when plant equipment is modified (e.g., a special model may be required for each type of plant equipment).

4.2.2 Portable Test Equipment

Test equipment may vary in the degree of portability; it may be as small as a hand-held voltmeter or as large as an engineering workstation. For example, the Westinghouse Eagle 21 Reactor Protection System features a rolling test cart that is used for surveillance tests and for adjusting setpoints and tuning constants. Essentially, it is an IBM-compatible personal computer on wheels (Galyean, 1994).

Portable test equipment may be connected internally or externally to the plant equipment. For example, some test equipment has probes that are manually positioned on the internal components of plant equipment for tests. Other

portable test equipment is connected to test ports on the outside of the plant equipment. For example, the portable ATE used with the Westinghouse Eagle 21 Reactor Protection System plugs into the Tester Subsystem of that system (Galyean, 1994).

Portable test devices may also plug into built-in test equipment (Hessburg, 1992).

4.2.3 Built-In Test Equipment

Built-in test equipment (BITE) is an integral part of plant equipment; it may be incorporated into a component, module, subsystem, or system. It may be as simple as a voltmeter, or as complex as an automatic checker (Wagner et al., 1996). The scope of BIT features may be partly determined by the digital system's size. For example, a single digital processor may contain a BIT feature that checks it for faults; large digital systems may have many devices to continuously ensure that its sensors, processors, and transmission components are operating properly. Many modern chemical and fossil-power plants equipped with distributed control systems have automatic, continuous test features that generate alarms whenever faults are detected in the system's hardware.

More sophisticated BIT features can retain historical performance information, diagnose failures, and display both the diagnosis and the instructions for corrective actions. Such systems have been used in aviation for some time. The following describes such features in F-15 fighter aircraft: "With the engine event history recorder, we are capturing critical engine events as well as events in the flight envelope that were in existence when the events took place. We are finding that this provides a very useful diagnostic tool beyond BITs. We can correlate what the airplane was doing at the time certain malfunctions happened" (Nondorf, 1992).

Some BITE can automatically execute corrective actions. Examples include digital systems with redundant processors, such as the fault-tolerant digital control systems described earlier that automatically switch control capability to a backup processor when the primary processor fails. More sophisticated digital systems may perform "self-repair" or performance-optimization functions. For example, the control system on the General Motors Northstar engine can change valve timing and cylinder firing to compensate for a complete loss of coolant. Also, BITE has been proposed as a way to allow combat aircraft to "self-repair" during battle (Maddox, 1996).

BITE has certain advantages compared to portable test equipment (Wagner et al., 1996; Bongarra et al., 1985):

- Less likely than portable equipment to be lost or damaged
- Available when needed (i.e., it does not have to be transported to the equipment that is to be tested)
- No special storage facilities are required

The disadvantages of BITE include the following:

- Likely to add to the weight and space requirements of the equipment being tested
- More test equipment is likely to be required when it is built-in, rather than portable, because a separate BIT device is usually required for each unit of plant equipment
- Transporting BITE to a point for convenient calibration may be more difficult than transporting portable test equipment
- Installing test equipment permanently may increase the complexity of the system's wiring and may even increase the need for maintenance

4.2.4 Display Formats of Test Equipment

Test results may be processed and presented to the maintainer in many ways. The following describes two presentation formats: go/no-go, and collating.

Go/No-Go Test Format – Go/no-go test equipment supplies one of two alternative answers to any question. The "go" response indicates an acceptable condition, and the "no-go" response indicates an unacceptable one. This format may be used to indicate whether a given signal is in or out of tolerance. The advantages of go/no-go test equipment include the following (Wagner et al., 1996):

- Presenting information clearly and unambiguously
- Simplifying difficult tasks, such as balancing circuits and checking complex wave shapes

The disadvantages include the following (Wagner et al., 1996; Bongarra et al., 1985):

- Requiring unique circuitry for each signal value to be tested (sometimes, however, ordinary displays can be converted to go/no-go displays by using reference scales, such as putting a colored band in the unacceptable range of a meter dial)
- Increasing the number and complexity of circuits required, which may add to initial cost and development time and increase the rate of breakdown of test equipment
- Providing relatively little help to the maintainer in checking common voltages or simple wave shapes because the go and no-go indications are presented rather than the actual values
- Requiring a special model for each unit of equipment that is to be tested

Many of these disadvantages may be lessened by using programmable test equipment in which acceptable ranges are predefined and preprogrammed for each unique test.

Collating Test Format – Collating test equipment shows the results of two or more checks as a single display. For example, a "test passed" light would come on only if all of the relevant signals are in tolerance (Wagner et al., 1996). An advantage is that it reduces the number of displays the maintainer must read, thereby reducing testing time and, possibly, errors. However, the disadvantages are similar to those for go/no-go test format.

4.2.5 Advanced Troubleshooting Aids

Industry experience in domains that extensively use advanced digital systems, such as military aviation, has shown that due to the complexity and difficulty of testing and troubleshooting, maintenance tasks may require advanced, computer-based troubleshooting aids. The introduction of such aids puts new demands on personnel, and is likely to require changes in maintenance practices, procedures, and personnel training.

The following describes two advanced computer-based aids that assist maintenance personnel in troubleshooting and repairing systems in the F-15 aircraft (Nondorf, 1992). The descriptions are examples of the types of aids that maintenance personnel in NPPs may be required to use in the future.

Wire Assessment and Repair Tool – This tool assists maintenance personnel in identifying electrical wiring. Wires usually are marked with identifying information at each end and at each connector, but not in between. Also, wires

sometimes are added to an aircraft, while non-functional ones may remain in place. Hence, maintenance personnel may have difficulty identifying wires and tracing their connections. The wiring assessment and repair tool is a computer-based simulation that creates wiring diagrams on-line, working backwards from a specified point. Once the maintenance technician has identified the wire harness, the system can identify the pin connections that should be tested. This information can be presented on a computer screen, or printed out.

Computerized Fault Reporting System – This system automates many of the steps for identifying a fault and producing the technical information needed to support the maintenance. Information is gathered from questions posed to the pilot. In addition, information is entered from the aircraft's maintenance-status panel and other locations. These data are processed using fault logic. The computer generates a 23-digit fault code that identifies the affected item and the technical information required for the repair. It also generates a work order, informs personnel in the maintenance depot of the problem, and orders the required parts from supply. If a part is removed from the airplane and sent elsewhere for the repair, the system maintains records. Each part is tracked individually to maintain a historical record of problems experienced and service received.

4.3 Maintenance Procedures

Maintenance test procedures may be paper based, incorporated into the computer-based test equipment, or a combination of both. Maintenance technicians may need aids to maintain awareness of test procedure status when multiple tests must be performed in a limited period. For example, Mittal, Bobrow, and De Kleer (1988; cited in Klauer et al., 1993) describe the interface of a troubleshooting device that displays plans in a graph-like format. Technicians can use a browse feature that shows the relationship of the current test to the overall test process and to the overall plant performance. Also, a history interface records interactions with the system.

4.4 Training Aids

Maintenance training aids include representations of equipment that personnel will be required to service. They provide trainees with experience performing maintenance tasks, and are especially important for developing troubleshooting skills. Maintenance training aids may range from simple bench mockups to complex computer-based simulations. Three types are described below: bench mockups, simulation-oriented computer-based instruction, and virtual-reality training aids.

Bench Mockups – A bench mockup is an actual unit of equipment or replica used in a training or maintenance environment for checking or locating faults. These mockups may have signal generators and dummy loads to simulate inputs and outputs (NRC 1985a, 1985b). They may be used to train personnel in troubleshooting, or to practice and refine maintenance activities before they enter the plant. Bench mockups often require additional equipment for their operations, such as signal generators and extra junction boxes, terminal strips, test points, controls, and displays.

Simulation-Oriented Computer-Based Instruction – Simulation-oriented computer-based instruction (SOCBI) provides trainees with a two-dimensional, interactive depiction of the particular equipment they are learning to troubleshoot (Maddox, 1996). This approach was started in the aviation domain in the late 1970s, and has been used in the nuclear industry. It exposes trainees to realistic failures by simulating the equipment's behavior. Trainees use this representation to practice diagnosing faults that are built into the simulation; they select tests and acquire information much as they would with the actual equipment. SOCBI systems may show graphical representations of the actual controls and displays used by maintenance personnel, or provide diagrammatic (i.e., logical) representations of a system. Functional and logical diagrams can illustrate how a system is functionally connected and allow trainees to use logical troubleshooting algorithms.

Virtual-Reality Training Aids – Majoros and Boyle (1997) describe the use of virtual reality (computer-generated representations of real-world objects) in training maintenance personnel. While SOCBI systems depict the behavior of equipment two-dimensionally, a virtual reality system can depict both the behavior and physical characteristics of equipment three-dimensionally. Trainees interact with virtual representations of equipment. These training aids have some advantages over physical mockups. For example, less space may be required to represent the task. Personnel can be trained for equipment that is not available or accessible, including equipment not yet built. Also, virtual reality can represent a larger part of the maintenance environment, such as surrounding equipment.

5 DEVELOPMENT OF THE TECHNICAL BASIS

This section identifies human performance considerations associated with maintaining digital systems. Section 5.1 provides a general discussion of the concepts of maintenance, maintainability, and human error. Sections 5.2, 5.3, and 5.4, respectively, discuss human performance considerations identified through reviews of industry experience, interviews with subject matter experts, and reviews of basic literature. These discussions center on factors that affect the performance of maintenance and may challenge plant safety. Section 5.5 describes aspects of human performance needing additional research before establishing review guidance.

5.1 General Concepts

5.1.1 Maintenance

Maintenance may be defined as "...a process with the objective of preserving the reliability and safety of NPP structures, systems, and components or restoring that reliability when it is degraded" (NRC, 1985a, p. 1). Preventive and corrective maintenance are distinguished. Preventive maintenance may be defined as "...regularly scheduled tasks (e.g., inspection, servicing, adjustment, calibration, replacement) intended to keep equipment in condition for operational or emergency use" (NRC, 1985b, p. B-1). Corrective maintenance typically refers to unscheduled maintenance undertaken in response to a malfunction or an indication of a failure.

Maintenance and surveillance are performed during all modes of NPP operation by plant personnel, vendors, and contractors and may include the following (NRC, 1985a):

- Diagnostic or periodic testing, surveillance, and inspection to determine the condition of structures, systems, and components
- Preventive and corrective actions, such as repair, replacement, lubrication, adjustments, or overhaul
- Proper equipment isolation, restoration to service, and post-maintenance testing to assure adequacy of corrective action

Simply, these categories may be summarized as testing, troubleshooting, disassembling and reassembling, servicing and adjusting, and replacing and repairing.

Testing and troubleshooting refer to examinations in which the operation of equipment is compared to performance criteria. A distinction may be made between testing and troubleshooting. Troubleshooting usually involves testing, but the term implies that some sort of fault (e.g., "trouble") is involved. Thus, troubleshooting may involve a series of tests and examinations to diagnose the cause of a failure and to locate the failed unit of equipment. However, testing can be unrelated to a suspected problem. For example, periodic tests, surveillances, and inspections make sure that a unit of equipment is operating within calibration tolerances (Maddox, 1996). After maintenance or repair is completed for a unit of equipment, acceptance tests may be performed to verify that the work was successful and the unit performs correctly. Such post-maintenance tests are similar to surveillance tests because they confirm that the equipment operates properly, rather that trying to isolate a problem. For digital systems, equipment functions are largely defined by software. It is difficult to detect faults by visually inspecting components, as in some analog systems. Therefore, testing and troubleshooting of digital equipment relies primarily on the use of electronic test equipment.

Disassembling and reassembling is often required for maintenance. It may be necessary to partially disassemble a unit of equipment to access internal components so they can be tested, serviced, adjusted, replaced, or repaired. As described in Section 4.1, digital equipment is susceptible to spurious signals and damage from handling. Thus,

digital equipment must be disassembled and reassembled carefully, such as when inserting and extracting printed circuit cards from slot connectors.

Servicing refers to routine maintenance tasks (e.g., cleaning, lubricating, filling, draining, and charging), and may be part of a preventive maintenance (PM) program. Adjusting refers to applying minor corrections to the operation of equipment, such as setting the value at which it will operate. In digital systems, components may not require the type of periodic servicing given to mechanical components that wear out, such as periodic lubrication and physical alignment. Nevertheless, software must still be maintained (modifying the stored instructions or data stored in computer files). This may have to be done for many reasons: software upgrades (e.g., installing the latest operating system), hardware upgrades (e.g., modifying software to be compatible with new hardware), and tuning the performance of plant systems (e.g., adjusting the parameters that control a system's behavior).

Replacement refers to the substitution of a piece of equipment for one that has failed. Repair refers to corrective action performed to restore a failed piece of equipment. For digital equipment, repair and replacement may involve hardware, software, or both. The replacement of larger units, such as printed circuit boards, may be performed locally in the plant. Smaller units of digital equipment, such as individual components on a printed circuit board, are likely to be replaced in a maintenance shop or at a vendor facility, due to their susceptibility to spurious signals and physical damage.

5.1.2 Maintainability

Maintainability (i.e., ease of maintenance) refers to the design of equipment to support effective and efficient maintenance. It is often described in terms of the ability of personnel to perform maintenance within a particular set of constraints, such as time and cost. Maintainability has been defined as follows:

> The measure of the ability of an item to be retained in, or restored to, a specified condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures and resources, at each prescribed level of maintenance and repair. (MIL-STD-721C, Definition of Terms for Reliability and Maintainability, 1981; cited in Majoros and Boyle, 1997, p. 1572).
>
> An inherent design characteristic dealing with the ease, accuracy, safety, and economy in the performance of maintenance functions. (Blanchard, 1986; cited in Majoros and Boyle, 1997, p. 1571).

Maintainability is related to the availability of equipment because equipment that is easy to maintain can also be returned to service more quickly. The degree to which ease of maintenance increases the availability of equipment can be expressed as follows (Majoros and Boyle, 1997):

$$A \quad \frac{R}{R\ M}$$

where:

A = availability (fraction of time that equipment is available for use)
R = reliability (average in-service time between failures)
M = maintainability (time to repair)

Watterson, Royals, and Kanopoulos (1992) expanded this equation for corrective maintenance by separating the maintainability term (M) into (1) time to detect and diagnose the failure, and (2) time to repair it. This is a valuable distinction because troubleshooting (fault isolation) is a major activity. On complex equipment, most corrective maintenance time is spent identifying faults (Majoros and Boyle, 1997). In NPPs, availability also is affected by

preventive maintenance, which can include the amount of time that equipment is out of service for surveillance testing and for preventive maintenance. Such preventive maintenance can be a major factor in reducing the overall availability of equipment.

Personnel performance can affect all of the factors related to availability. For example, while the time between failures of a unit of equipment (R) is usually associated with such factors as the design of the equipment, operating conditions, and the operating environment, it can also be affected by the performance of maintainers, since improper maintenance can cause immediate or premature failures. The time required to repair equipment (M) is affected by the ability of maintenance personnel to correctly and promptly detect, diagnose, and then fix the failure. Thus, availability is affected by the ability of maintenance personnel to quickly and correctly perform corrective maintenance, surveillance tests, and preventive maintenance.

The availability of equipment is directly related to plant safety. If equipment is unavailable because it has failed or is being serviced, then plant safety or risk is affected by the amount of time that the safety functions of that equipment are not available. When a single component is out of service for maintenance, the increased risk may be expressed as follows (Samanta, Kim, Mankamo, and Vesely, 1994):

$$r_m \quad R \bullet d_m$$

where:

r_m = single-event risk contribution from maintenance of component in question
R = increase in risk (core damage frequency) when component is down for maintenance
d_m = downtime associated with the maintenance

The risk measure can be core damage frequency, severe accident frequency, an expected consequence level, or even a system unavailability level. The plant's probabilistic risk assessment (PRA) can be used to calculate the R value. The maintenance in question could be either periodic preventive maintenance or corrective maintenance event due to equipment failure. The yearly contribution to risk can be determined by incorporating into the equation the scheduled frequency of the preventive maintenance or the failure rate of the component for corrective maintenance events. The equation for the preventive maintenance case then becomes:

$$R_m f_{pm} \bullet \; R \bullet d_m$$

where:

R_m = yearly risk contribution from preventive maintenance of the component in question
f_{pm} = yearly frequency of preventive maintenance on the component

The corrective maintenance equation is similar with the component failure rate (f_r) substituted for f_{pm}:

$$R_m f_r \bullet \; R \bullet d_m$$

In addition, both the failures of equipment that have not been adequately maintained and personnel errors that occur during maintenance can initiate transients. Increases in the frequency of these initiating events can also affect plant safety; the effect on risk can be calculated by using the changes in the frequency values of the pertinent initiators in the PRA.

In summary, the availability of plant equipment is affected by personnel performance associated with all of the categories of maintenance activities discussed (i.e., testing, troubleshooting, disassembling and reassembling,

servicing and adjustment, and replacing and repairing). Changes in availability directly affect the plant's risk as determined by the plant-specific PRA.

The focus of this report is on maintainability features of digital systems that affect the performance of maintenance personnel. This includes factors that affect the ability to quickly and accurately carry out periodic surveillance, preventive maintenance, and corrective maintenance. Equipment that is not adequately designed to support maintenance may delay completion of preventive or corrective maintenance, or may cause maintenance personnel to make errors, both of which may reduce the availability of plant systems and increase risk.

5.1.3 Testability

The following discussion is derived from Bennetts (1984), who provides useful discussions of testability and other concepts related to maintaining digital equipment. The amount of time required to detect and diagnose a failure depends, to some degree, upon the complexity of the test and the ease with which it can be performed. Tests may range from a simple continuity check (i.e., a verification that a circuit is not open) to a complicated evaluation of an electrical system's response to a specific pattern of inputs. Testability relates to the ability to develop and apply tests to satisfy predefined levels of performance (e.g., detection and isolation of faults) within constraints, such as cost and time, and is one of the considerations of overall maintainability. Thus, if the cost of testing a design is excessive, then for practical purposes, the design cannot be tested.

Traditionally, the two disciplines of logic design and test program development were separated. First, the designers created the circuit logic. Then, the programmers developed test programs to detect or isolate faults in the circuit. However, the increasing complexity of digital circuits soon led to designs that, for practical purposes, were virtually not testable. It is now recognized that testability must be included in the design process.

The primary objective of testing digital circuits, at the chip, board, or system levels, is to *detect* failures, including hardware faults caused by problems in manufacturing, operating stress, and wear. Since the main concern is to determine whether a fault is present, this may be referred to as go/no-go testing. The secondary objective of testing is to locate the cause of a fault with enough precision to allow its repair to be carried out. This *diagnostic* testing involves both detecting and locating the fault. Diagnostic testing applies to equipment designed to be repaired.

Circuit testing entails applying a stimulus signal to the circuit, observing the response, and then comparing it to a fault-free response pattern. Normally, a circuit can only be stimulated (driven) through certain access points, such as pins on integrated circuit chips or edge-connector fingers on printed circuit boards. Similarly, the circuit usually can only be sensed (monitored) at other specific access points. Inputs that can be driven are called primary inputs, and outputs that can be sensed are called primary outputs.

Testing may be described in terms of three major activities: generating, evaluating, and applying tests. Tests may be generated and evaluated by designers during the design process or by maintenance personnel when installing and maintaining the equipment. Tests are applied by maintenance personnel during both processes.

Test generation is the process of developing a set of primary inputs and their expected fault-free responses. These are developed for a target fault list – a set of faults to be addressed by the tests. Two factors affect the ease of generating tests: (1) the degree to which the circuit is controllable (e.g., through the range of possible test signals and access points for primary inputs) and (2) the degree to which the circuit is observable (e.g., through the available access points for primary outputs). When these features are not adequately built into a circuit, it is difficult to create the right circumstances to excite and propagate fault conditions. Test generation also may be difficult for printed circuit boards and other devices that use stored-state devices within complex feedback structures. The more complex the structure, the more difficult it becomes both to control and to observe the behavior of the circuit. For designs using bus structures, the problems in formatting tests are more closely related to understanding the

complexity of LSI and VLSI devices than to controllability and observability. Some specific problems include inadequate technical information and a lack of knowledge of the precise ways in which the devices can fail.

Test evaluation is the process of evaluating the primary inputs and expected fault-free primary output responses to ensure that the test set adequately covers the range of faults identified in the target fault list. One method for evaluating tests is to physically insert faults into good devices or printed circuit boards, and then check to see that the tests can detect or diagnose the faults. However, this method is limited by such factors as the lack of access to integrated circuits and also that the physical faults must be limited to those that do not damage other parts of the device. Another method is to simulate the faults using a software model of the circuit; this is called a logic fault simulator. Faults may be selected from the target fault list and inserted into the model – individually for serial fault simulators, or in predefined groups for parallel fault simulators. A limiting factor in simulations is the ability of programmers to develop a model that accurately represents the behavior of the circuit. This inability may be due to inadequate technical information, device complexities and differences, and unknown failure mechanisms.

Test application is the process of physically applying the tests to the real circuit. Problems can stem from the limitations of ATE, such as maximum test rates and restrictions on fault dictionaries and other testing features. Another problem is physical access and interfacing requirements, especially where devices on boards are physically close to each other, or test programs require additional access through non-standard leads. Test application can also be difficult when faults must be isolated, particularly for circuits that have global feedback structures in which the cause-effect relationship cannot be resolved around a closed loop.

All three phases, test generation, test evaluation, and test application, can affect the performance of personnel maintaining digital systems. Test application includes most of the tasks of maintenance personnel – detecting and diagnosing failures in digital equipment. Test generation and evaluation may be undertaken by either design or maintenance personnel. In either case, these activities have important effects on maintenance personnel because deficiencies in generating and evaluating tests can result in equipment that cannot be adequately tested, or test sets that do not thoroughly evaluate the equipment.

5.1.4 Human Error in Maintenance

Many theoretical analyses of human error exist with varying classifications of error types. One widely accepted scheme divides errors into two major categories: mistakes and slips (Lewis and Norman, 1986; Norman, 1981, 1983; Reason, 1990; Reason and Maddox, 1996), based on consideration of intention. An intention is a high-level specification that starts a chain of information processing, which normally results in accomplishing that intention (Norman, 1983). An error in the formation of an intention, such as forming an inappropriate one, is called a *mistake*. An error in carrying out an intention is called a *slip.*[2]

Mistakes are due to incorrectly assessing the situation or inadequately planning a response. The main sources of information used by maintenance technicians for their tasks include displays and controls at the maintenance site, labeling and other physical characteristics of the equipment to be maintained, information from operations personnel, procedures, technical support documents, and test equipment. From these information sources they make decisions about the state of the plant, its systems, and equipment. This is important for selecting tests, interpreting results, diagnosing and isolating malfunctions, selecting maintenance actions, confirming that they were carried out properly, and verifying that the equipment operates properly afterwards. Mistakes made during maintenance include formulating incorrect or inadequate plans, such as planning the wrong test or repair, or failing to consider the full range of consequences of the planned maintenance. For example, a maintainer may correctly conclude that a component should be tested but then select the wrong rule for the test. As another example, a maintainer may

[2] Reason (1990) describes an additional type of execution error called a *lapse*, which will not be addressed in this report.

incorrectly conclude from test results that component A should be replaced, when, in fact, it is functioning properly, or, a maintainer may correctly conclude that component A should be replaced, but fail to consider how its replacement may affect other system components.

Slips may take many forms during maintenance. They may involve the maintainer's interactions with the plant's equipment, or with support equipment, such as procedures, technical support documents, and test equipment. A schema is a sequence of linked behaviors that, through repeated performance or deliberate training, becomes somewhat automatic to the individual; that is, the behavior can be performed without focusing a great degree of attention on it. To control behavior, a schema must be first activated in memory and then triggered into action. This occurs whenever the schema's activation value and the goodness-of-match of its trigger conditions reach their threshold levels (Norman, 1983). Slips result from "automatic" human behavior when schema (i.e., subconscious actions intended to accomplish the intention) get waylaid en route to execution. Thus, while one action is intended, another is accomplished. Lewis and Norman (1986) state that, on the whole, people can consciously attend to only one primary thing at a time. They can do many things at once only if most of the actions are automatic (subconscious), with little or no need for conscious attention. Thus, conscious attention often is focused at high levels while low-level physical movements are controlled subconsciously. This lack of attention may result in incorrect activation and triggering of schemas, which produce slips.

Slips may include improperly executed actions during periodic surveillances, troubleshooting, diagnosis and isolation of malfunctions, installations, adjustments, repairs, replacements, and verifications of proper operation of equipment after maintenance. For example, a maintainer may perform the intended test but may inadvertently read or record the results incorrectly. As another example, a maintainer may intend to install printed circuit card A into slot B but install it into slot C instead.

5.2 Industry Experience: Failures of Digital Systems

The following describes human performance considerations associated with maintaining digital systems that were identified by reviewing industry experience. Section 5.2.1 discusses reviews by the NRC, Section 5.2.2 presents an analysis made by BNL, and Section 5.2.3 discusses findings from analyses of international incidents.

5.2.1 NRC Reviews of Digital System Failures in U.S. NPPs

In ensuring the safe operation of nuclear reactors in this country, the NRC reviews operational events related to digital systems. The following describes findings from some of these reviews.

5.2.1.1 NRC Information Notice 93-49

In Information Notice 93-49, Improper Integration of Software into Operating Practices (NRC, 1993), the NRC's staff reviewed four events that occurred in software-based digital systems of NPPs. The first event was a time-delay error detected in the actuation circuitry of the anticipated-transient-without-scram (ATWS) mitigation system. This incident was attributed to a vendor's technician loading an uncontrolled version of software into a hard drive that had just been installed. This improper version rebooted (restarted) the system incorrectly.

The second event involved a failure of an annunciator driver, which caused the overhead annunciator system in the control room to be inadvertently configured so that it did not update the annunciators to indicate the true alarm status. The overhead annunciator's design allowed an operator using a remote workstation to place an event recorder in a mode other than the usual operating mode, and then enter password-protected software, without encountering warning messages. The incorrect mode was accessed when a switch was wrongly positioned. Then an operator, who was attempting to obtain data on system status, miskeyed the characters of a command that happened

to be a valid command in the accessed mode. This resulted in an unauthorized manipulation of the system, and so placed the overhead annunciator system in the undesirable configuration.

The third event, a failure of the diverse scram system, occurred when an I&C technician attempted to clear some alarms by rebooting the system's control processor. It was determined that the reboot was improper and rendered the diverse scram system inoperable.

The fourth event involved an inoperable torus temperature monitoring system. The licensee found that three out of twelve circuit cards in one channel had defective solder joints. The cards were replaced and the channel was declared operable. Subsequent checkouts showed that the programming of a module in this channel was loaded with an incorrect software algorithm that resulted in potentially non-conservative output. This problem was addressed by loading the correct software.

The NRC described these events as examples of how inadequate integration of software-based digital systems into operating practices, and inadequate knowledge of the intricacies of software-based digital systems by technicians and operators caused systems to become inoperable. Using these examples, the NRC noted that software-based digital systems are susceptible to failure modes different from those of analog systems or hardware-based digital systems.

5.2.1.2 NRC Information Notice 96-56

Information Notice 96-56, Problems Associated with Testing, Tuning, or Resetting of Digital Controls While at Power (NRC, 1996) describes reactor transients, reactor trips, and actuations of engineered safety features caused by testing, tuning, and resetting digital controls while the plant is at power. The NRC reviewed four events. In the first event, testing of a recently installed digital adjustable-speed-drive modification to the reactor recirculation pumps caused a rapid change in reactor power of 15 percent within 40 seconds. This event was attributed to a keyboard (soft control) error in the set point of the reactor recirculation flow. A test engineer intended to type a setpoint value of 51 percent, which an operator could execute, if needed, by pressing the "Enter" key. However, the test engineer inadvertently transposed the digits (e.g., typed 15) and then pressed the "Enter" key. The error was immediately recognized and the instruction corrected. This caused the rapid decrease and then increase in reactor power.

In the second event, an NPP operating at 45 percent power experienced a loss of reactor feedwater control and a subsequent decrease in the reactor vessel's water level while changing an on-line configuration to accommodate a recently installed digital feedwater control system. The event occurred after a minor change in software logic was inserted into a backup control module, and the module was placed in the execute mode. A subsequent design review found an error in the logic execution sequence in the original firmware that would have closed a feedwater regulating valve any time the backup control module attempted to take control from the primary control module in the automatic mode.

In the third event, an NPP operating at full power experienced an automatic reactor scram on low reactor water level. The low level resulted from an unexpected runback of two of the three reactor feedwater pumps, which occurred while software parameters were being changed in a recently installed digital feedwater control system. The cause of this event was attributed to inadequate design of the control system's software. The design weakness, unknown to plant personnel, caused the control system to automatically reinitialize to zero output when parameters were changed in certain software blocks. This drove the feedwater pump's speed-demand signal to zero for a few seconds.

In the fourth event, an NPP experienced an automatic start of the motor-driven auxiliary feedwater pumps while personnel were resetting the central processing units in the digital main feedwater pump turbine control system. While I&C technicians and a vendor's representative were resetting the third of three central processing units, an inadvertent trip signal was generated for two feedwater pumps caused by their having inadequately restored the

second central processing unit before rebooting the third unit. The main feedwater trip signal was generated because the system sensed that two of the three central processing units were not functional.

The NRC stated that these events demonstrate that resetting processors in digital control systems or manipulating software on-line as part of tuning or testing of digital control systems can result in unforeseen transients, reactor trips, and actuations of engineered safety features. These events highlight the importance of evaluating proposed changes and developing and implementing controls for any type of on-line manipulation of digital control systems. Such administrative controls are needed to minimize potential errors and to develop awareness of the potential effects of these errors.

5.2.1.3 Review of Digital System Failures: NRC's Office of Analysis and Evaluation of Operational Data

The NRC's Office of Analysis and Evaluation of Operational Data conducted a study to identify the types of digital system failures that have occurred in the U.S. NPPs (Lee, 1994). Their study included 79 licensee event reports (LERs) on computer-based digital system failures from 1990 to 1993. Four categories of failures were defined: Software Error, Human-Machine Interface, Electromagnetic Interference, and Random Component Failure.

Any event caused by a software failure was categorized as a Software Error; these were further separated into verification and validation failures, and configuration control failures. The Human-Machine Interface Error category was defined as any event caused by a digital system failure attributable to human error, including "...unauthorized computer data entry, deviation from procedure, and inadequate procedures for plant personnel" (Lee, 1994, p. 3). Clearly, many software verification and validation failures and configuration control failures also are caused by human error. However, these were counted in the Software-Errors category, and not the Human-Machine category. Thus, Lee considered only those errors that occurred during plant operation and maintenance, and not errors that occurred during the design. The Electromagnetic Interference category was defined to include any event caused by electromagnetic interference, poor grounding, or poor connections. The Random Component Failure category included any event caused by a random failure of a component.

The distribution (number/percent) of failures was as follows:

- Software Error – 30 (38%)
- Human-Machine Interface Error – 25 (32%)
- Electromagnetic Interference – 15 (19%)
- Random Component Failure – 9 (11%).

Thus, software errors and problems with the human-machine interface accounted for approximately 70% of the reviewed incidents.

5.2.1.4 Review of Digital System Failures: NRC's Instrumentation and Controls Branch

A separate review covering the years 1987 to 1996 was conducted for the NRC's Instrumentation and Controls Branch by Ganiere,[3] using a categorization scheme similar to that used by Lee (1994). One notable exception was that the category that covered events involving the human-machine interface (i.e., the control room HSI), was not restricted to human errors. Thus, some events in this category resulted from causes other than the actions of

[3]Ganiere, J. (1997). (Draft findings from an unpublished study by the U.S. Nuclear Regulatory Commission). These events also appear in a series of reports on failures of computer-based digital systems issued by the NRC I&C Branch (Wemiel, 1997a and b; 1996a, b, c, and d; and 1995a, b, and c).

operators or maintenance personnel, such as equipment deficiencies. Ninety-two failures were identified, some of which were also discussed by Lee. The distribution (number/percent) of failures was as follows:

- Software Deficiencies – 40 (43%)
- Human-Machine Interface Problems – 14 (15%)
- Electromagnetic Interference Problems – 9 (10%)
- Random Hardware Component Failures – 29 (32%).

As in Lee's review, Ganiere found that software problems were a leading cause. A notable difference is the higher percentage of events he attributes to random component failures; Ganiere attributed about 32% of events to "random hardware component failures" while Lee attributed only about 11% of them to it.

5.2.2 Incidents Related to the Maintenance of Digital Systems

5.2.2.1 Review of Event Reports

BNL subsequently reviewed those events related to digital systems that were identified by Lee (1994) and Ganiere (see Footnote 3), focusing on events involving maintenance and identifying the underlying human performance considerations. From Lee's descriptions of the failures assigned to the Human-Machine Interface Error category, 16 were considered to be maintenance related. The remaining events in this category were not examined further because they either were related to operations, or there was insufficient information to relate them to maintenance. One event, caused by the actions of operators during normal operations, was included because it resulted from the use of a console that is usually used for maintenance and system configuration activities. In addition, two events included in the Electromagnetic Interference category were caused by incorrect reassembly of digital equipment during maintenance, and therefore, were considered maintenance-related. Thus, 18 maintenance-related events were identified from the Lee (1994) study.

Of the 14 events included in the Human-Machine Interface Problems category by Ganiere, one was primarily due to a software design defect; it was excluded from further consideration. The remaining 13 events were considered maintenance-related. Among the 18 maintenance-related events from Lee's study and the 13 from Ganiere's study, 3 were duplicates. Eliminating the duplicates gave a set of 28 events related to maintaining digital systems; they spanned the years 1990 to 1996.

Descriptions of the 28 events were reviewed further to identify causes; many had more than one. The events were organized into the following categories: Procedure-Related, Input Errors, Assembling, Testing, and Other to indicate a primary cause (Table 5.1).

Table 5.1 Causes of Events Associated with Maintenance of Digital Systems

Procedure-Related (12)

- Failure to follow the out-of-sequence situation procedures led to a reactor trip resulting from a general warning alarm on both trains of the solid state protection system.
- Inadequate procedures allowed the setpoint limit to be set at a lower level.
- Inadequate change procedures for a database manual caused the setpoint of a wide-range gas monitor to be set incorrectly.
- Failure to follow procedures when entering the computer data led to a special condition surveillance being missed.
- Lack of administrative control during troubleshooting led a technician not to return the process computer's point to scan, causing the plant computer's point to go out of scan.
- Procedural deficiency led a technician to miss bypassing the trip signals while preparing to test a reactor protection system.
- Inadequate documentation of computer's operation led to an inadvertent bypass of the computer's rod-position deviation alarm, preventing the alarm from annunciating.
- Lack of a work document or procedures for controlling an adjustment led to incorrect keypad entry, which caused the analyzer not to operate.
- Procedures did not test the entire component circuitry which led to missing the required surveillance, causing a violation of technical specifications.
- While rebooting one of three central processing units, an inadvertent trip signal was generated for both feed pumps. It was caused by inadequate restoration of the second central processing unit before rebooting the third unit. Having two central processing units out of service generated a main feedwater pump trip signal. (Maintenance personnel failed to wait a specified amount of time after restoring the second central processing unit.)
- A human error occurred while installing a backup microprocessor in the digital feedwater control system due to insufficient vendor instructions for the special installation of the microprocessor. This resulted in feedwater transient and reactor trip.
- Improper rebooting in the intelligent control processor of the non-nuclear-safety digital automation control system rendered the diverse scram system inoperable. (Inadequately trained maintenance worker failed to properly follow the rebooting procedure.)

Input Errors (11)

- Incorrect entry on the computer scheduler program led to a required surveillance being missed.
- Incorrect data value input to diagnostic software caused an inappropriate torque-switch setting.
- A non-licensed test engineer typed an incorrect computer instruction and mistakenly entered the instruction causing a decrease in the reactor's recirculation flow and power.
- While returning the computer of the core-operating-limit supervisory system to service after maintenance, a technician entered the wrong date into it resulting in an erroneous core burnup value and rendering the core-operating-limit supervisory system inoperable.
- Eight programmable sensors for the containment hydrogen monitor were updated with the wrong temperature compensation coefficients.
- Incorrect data were entered into the computer database resulting in a non-conservative permit release setpoint on the liquid waste radiation monitor. (Deficiencies in the software design were also identified.)
- The containment hydrogen monitor became inoperable because incorrect calibration constants had been entered into the post-accident containment hydrogen monitor computer.
- The temporary annunciator system computer locked-up after an incorrect command was entered at the maintenance console.
- The temperature monitor became inoperable due to incorrectly entered software. (Two channels were inadvertently assigned to the same detector.)
- An inappropriate setpoint entered into the digital electrohydraulic turbine control system rendered the fast-open function of the main turbine's bypass valves inoperable.
- An operator inadvertently accessed password-protected software and performed unauthorized system manipulations causing a loss of the overhead annunciator system.

Table 5.1 Causes of Events Associated with Maintenance of Digital Systems (contd.)

Assembling (2)
- Loose and dirty microprocessor pin connections caused a relay failure, which led to containment ventilation isolation.
- Poor electrical connections of one or more plug-in integrated circuits in the analyzer caused an inadvertent actuation of control room ventilation.

Testing (1)
- A technician mistakenly connected digital multimeter input to the wrong system, which caused a reactor core isolation.

Other (2)
- A high-flow scram signal was generated during troubleshooting of the computer for the reactor's recirculation flow control system due to personnel error.
- Electrical perturbation caused by a technician's error caused a gas monitor channel to fail (leading to an Engineered Safety Feature actuation).

The Procedure-Related category contains the largest number; it includes 12 (43%) of the 28 events. These were due to inadequate procedures, the failure to follow procedures, or possibly both. Caution may be in order when considering events attributed to a failure to follow procedures because the description may obscure other factors that influenced personnel performance. For example, a failure to enter data as specified by a procedure may be due to the inadequate design of the interface used for entering the data.

The Input Errors category contains 11 events (39%) involving entering commands or data via a keyboard. Guidance addressing errors in data and command entry already has been developed for the hybrid HSI project for the topic, Soft Controls (Stubler, O'Hara, and Kramer, 2000). NUREG-0700, Rev. 1 also has general guidance on human-computer interfaces, which is also relevant to preventing input errors. Therefore, this topic is not discussed in great detail in this report.

The Assembling category included two events (7%) that were due to improper electrical connections; these were identified in Lee's Electromagnetic Interference category. Testing contained one event (4%) attributed to improper testing that occurred when a technician mistakenly connected a digital multimeter input to the wrong system. The Other category has two events (7%). The first event occurred because neither the maintenance personnel nor the control room operators noticed that the system being maintained had automatically transferred control to another redundant processor. This event might have been due to inadequate HSI design (i.e., indications of processor status were not sufficiently salient) or to a procedure-related problem (e.g., personnel failed to monitor indications properly). Because the relative contribution of these and other factors could not be determined from the description, the event was placed in the Other category. (This event is discussed further under the heading, "Event 1," in the discussion of on-line maintenance, below.) The second event was so assigned because the description did not provide details about the technician's error. In the event report (LER 50-311/90-008, 1990), it was surmised that the technician had inadvertently caused an unspecified electrical perturbation, which locked up a microprocessor that was interconnected with other systems, which ultimately led to the Engineered Safety Feature actuation.

Further analysis of selected events from Table 5.1 identified two types of digital system failures resulting from maintenance errors that are particularly affected by human capabilities. The first includes failures of computer-based systems that give little indication of their failed state. The second is failures that occur during on-line maintenance. Each is described below.

Failures That Provide Limited Indication of Their Failure State – Computer-based digital systems operate based on instructions provided by their software. Some maintenance errors can change the instructions or the way the computer processes them. The computer system may show little indication that it is not operating or is operating improperly. These types of failures may be introduced during two conditions: installing the software and rebooting the computer. Examples are given below:

- *Software installation* – A programming error entered by a technician when installing an electrical, environmentally qualified, temperature monitor rendered that system inoperable. This condition was not discovered until two weeks later when an operator discovered that one channel was indicating an incorrect value. Subsequent investigation revealed that manual entry of software had been necessary during the installation due to incompatibilities between systems, and in doing so, two channels were inadvertently assigned to the same detector. A line-by-line review of the change by the technician and the vendor did not detect the error. The technician retesting the upgrade did not detect a difference of 27 F between the "as found" and "as left" data for the inoperable point. The root cause of this event was determined to be personnel error – the technician incorrectly entered the software and then failed to detect the error when reviewing its installation (LER 50-423/93-008, 1993). This event reveals three human performance problems. The first was a susceptibility to errors when entering data manually; the system apparently was not designed to show an error message when the two channels were incorrectly assigned to the same detector. The second problem was the difficulty in detecting software errors by inspecting code line-by-line. The third problem was the difficulty in detecting incorrect operation of the system once it was in service.

- *Restart of a computer-based control system* – When flashing trouble indications appeared on the intelligent, non-nuclear safety, digital automation-control system, an I&C technician attempted to clear the alarms by rebooting the control processor, and thereby rendered the diverse scram system inoperable. On the following day, it was found that the system had been inoperable since the reboot. The cause of this event was attributed to inadequate training of the technician (NRC, 1993). However, the event also indicates the susceptibility of digital systems to improper actions during restart, and the lack of feedback to personnel when errors are made. After the processor was improperly rebooted, it was not apparent that the diverse scram system was inoperable.

Failures that Occur During On-Line Maintenance of Digital Systems – Digital system upgrades for I&C equipment often feature redundant processors, which allow maintenance to be performed while the plant is operating at power (NRC, 1996); one processor typically is serviced while a redundant one controls the system. These digital systems are complex, having multiple processors and operating modes. Furthermore, because maintenance occurs while the plant is operating, errors can have important safety consequences. On-line maintenance imposes special demands on personnel as they must understand the structure and operation of these complex systems, maintain awareness of changes in the systems' status and behavior, and understand how maintenance can affect these systems, and ultimately, the entire plant. Adequate HSI design and maintenance procedures are critical to supporting on-line maintenance. The following describes events in which HSI design and maintenance procedures played important roles in on-line maintenance:

- *Event 1* – The following event illustrates the complexity of digital systems, including redundant processors and multiple modes, and the effects they have on on-line maintenance; e.g., they impose new demands on personnel for maintaining awareness of system's status. It also illustrates the role of displays, alarms, and warning messages for enhancing situation awareness and preventing maintenance errors.

  In this event, a lack of awareness of the state of a redundant digital control system led to a trip of the reactor's recirculation flow control system. This system has two redundant computers: DCC-X and DCC-Y. Initially, DCC-X was in control, while DCC-Y was in an off-line diagnostic mode. The DCC-Y was being used as an aid by I&C technicians who were troubleshooting and repairing a wiring problem in transferring the control-logic circuit of the digital reactor recirculation-flow-control system. While wiring repairs were in progress, the DCC-

X computer tripped into the inactive state, which transferred the control of the speed of the recirculation pumps to the DCC-Y computer. Because this was a bumpless transfer, neither the I&C technicians nor the control room operators noticed it. When the dual-computer-failure alarm sounded for this system, the control room operators incorrectly assumed that the alarm was caused by the ongoing maintenance and had no potential affect on the operation of the recirculation pumps. As a result, the DCC-Y was allowed to control the recirculation pumps' speed while in the off-line diagnostic mode, without the I&C technicians or the control room operators knowing. The DCC-Y computer decreased the pumps' speed to 35 Hz, which was the last value retained by that computer before it was taken off-line. The operators made several attempts to increase the speed to 40 Hz via a master recirculation flow controller, but were unsuccessful. Exiting the off-line diagnostic mode on DCC-Y lowered speed demand to near 0 Hz, which was followed by a high speed demand (caused by the higher setting of the master recirculation flow controller). This large error signal caused the recirculation pumps' speed to over shoot, resulting in a recirculation flow exceeding the high flow scram setpoint; this caused a reactor scram (LER 50-219/94-021, 1994).

This event suggests that the HSI may not have provided adequate feedback to maintainers and operators to support on-line maintenance. In particular, it indicated the need for salient indication of the control systems' status and error messages that are appropriate for the control system modes. Neither the interface between the I&C technicians and the digital system, nor the interface between control room operators and the digital system allowed personnel to recognize that the DCC-X computer had tripped, and control of the system had been transferred to the DCC-Y computer. Because personnel were unaware of this transfer, and continued to try to control the system without noticing that their actions were ineffective, this constitutes a mode error (Stubler, O'Hara, and Kramer, 2000). This situation was further complicated by the fact that the DCC-Y computer was in a special mode – the diagnostic mode. When the I&C technicians exited the diagnostic mode, the recirculation pump speed controllers initially received a signal of almost 0, and then a signal for 40 Hz from the master controller. Thus, the I&C technicians' action of exiting the diagnostic mode had the effect of entering a very large error signal into the control system; the interface between the I&C technicians and the digital system apparently provided no warning that this would occur.

- *Event 2* – The following event illustrated the importance of adequate technical instructions when maintaining digital systems on-line. It also demonstrated the complexity of digital systems and their susceptibility to mode errors and complex interactions. In this event, insufficient special instructions from the vendor for installing a microprocessor in a digital feedwater control system resulted in a maintenance error that led to a feedwater transient and a reactor trip.

  In this plant, the digital feedwater control system automatically controls feedwater flow to the steam generators to maintain proper levels by adjusting control valves and the speed of the feedwater pump. Processor redundancy is implemented in the digital feedwater control system using a masterless scheme; either of the processors can operate as the primary one while the remaining processor is in backup mode. If the primary processor fails, a bumpless transfer to the backup occurs.

  Engineering personnel were installing a backup processor in the plant's digital feedwater control system while the plant was at 100% power. As it was inserted, the redundant processor, which was controlling the feedwater system, failed. This caused the main feedwater-system and all steam-generator controls to automatically switch to the manual mode, and drove several control room indicators for one steam generator (1A) to zero. This led the control room operators to believe that the main feedwater flow was lost, so they opened a main-feedwater valve to restore flow. When a high-high level alert for that steam generator annunciated, the operators realized that the main feedwater flow had not been lost and they began to close the valve. The resulting transient caused a low-low level alert for the affected steam generator, and then a reactor trip.

A few hours later, the reactor was in hot-standby mode, main feedwater pump 1B was tripped, and engineers were trying to restore the digital feedwater control system. They noticed that speed control of the main feedwater pump 1A had switched to its backup output card, which, at that point, was in the manual mode. An on-screen message showed that the backup output card was not in automatic mode. However, other indications, which normally occur at the engineer console during a switch to the backup control card or when a fault message is indicated, were not present. So, the engineering personnel proceeded to switch control back to the primary output card, unaware that the backup output card was in the manual mode.

When control was returned to the primary output control card, a bump occurred in the demand signal to the main feedwater pump 1A. Apparently, when the backup output card is in the manual mode, the signals of the primary output card are not matched with those of the backup output card to prevent a large difference. This bump caused the speed of the main feedwater pump to increase suddenly, tripping main feedwater pump 1A due to high discharge pressure. Because both the 1A and 1B main feedwater pumps were now tripped, an automatic start of the auxiliary feedwater system occurred.

These incidents were attributed in the LER to the failure of the vendor to provide special installation instructions. Had they been provided and used, (1) the redundant processor would not have failed, and (2) the full set of indications associated with the backup control card being in manual mode would have been provided at the engineer console (LER 50-413/93-008, 1993).

This incident is an example of on-line maintenance performed on a redundant digital processor without adequate instructions from the vendor. Lacking them, both the primary and secondary processors failed. The plant trip resulted from the operators' incorrect situation awareness; that is, faulty indications of feed flow led operators to conclude, incorrectly, that a large manual control action was needed. The resulting feedwater transient tripped the plant. The automatic start of the auxiliary feedwater system, which occurred later, was the result of a mode error on the part of the engineering personnel, who failed to notice that the backup card was in the manual mode, despite an on-screen message to that effect. Thus, this event points out the importance of adequate procedures for on-line maintenance of digital systems. It demonstrates that one incorrectly performed maintenance action may affect other components of the digital system and thereby complicate the event.

- *Event 3* – The following event illustrates the importance of following maintenance procedures during on-line maintenance. While rebooting one of three central processing units of a main feedwater control system, an inadvertent trip signal was generated for two feed pumps. This was caused by inadequate restoration of the second central processing unit before rebooting the third unit. Maintenance personnel apparently did not wait the requisite amount of time after rebooting the second central processing unit. Having two central processing units simultaneously out of service generated a main feedwater pump trip signal (NRC, 1996). This event is also interesting when contrasted with the reboot event described earlier. Unlike that event, the improper reboot did not result in a failure that provided limited indication of its failed state. Instead, it caused an immediate trip.

5.2.2.2 Plant-Incident Review

Brookhaven National Laboratory also reviewed incidents reported in a condition-reporting system of a U.S. PWR NPP. Although the scope of this review was limited (i.e., one NPP for one year), these incidents identify design characteristics and human performance considerations relevant to maintenance at other plants. Incident reports were sorted by title to identify those involving human errors associated with only the maintenance, surveillance, or testing of I&C systems. Seven incidents involving *digital* I&C systems were identified for the 1997 calendar year. They are represented by the following:

- Accidental operation of a component on the wrong circuit card resulted in inadvertent alarm actuations. (2 incidents).

- A motor-operated valve trip coil was incorrectly set at 3 instead of 1 because the technician misread the work order. This resulted in an instantaneous trip setpoint that was higher than desired.

- Technicians working on one channel of a steam generator level transmitter system accidentally took two of four channels out of service because they were unaware that the components were in different loops. This resulted in a steam generator low-low alarm, and movement of several valves.

- Electrical leads that were not connected in an electrical cabinet due to an incorrect wiring diagram resulted in an inoperable annunciator.

- Cable-jacket insulation for a resistance temperature detector in the reactor cooling system (RCS) was accidentally cut during a sleeving operation.

- During post-maintenance testing of switchgear, the overcurrent ground relay was accidentally bumped with test equipment, causing an unintended circuit breaker trip.

The first bullet represents two incidents that occurred when digital circuit boards were serviced. Because circuit boards are small (compared to analog circuitry), similar looking components responsible for different functions were located near each other. During maintenance, the wrong components were operated. In the first incident, a maintenance technician was inspecting circuit-card fuses. After one steam generator pressure loop was removed from service, the technician placed the switches on card B4-429 of card frame 4 into the "Test" position per the procedure. The next step required the technician to move to card frame 2 and place the switches in relay card B4-235 into the "Test" position. However, instead of moving to card frame 2, the technician moved to card B4-435, located in card frame 4. He momentarily moved a containment pressure bistable trip switch, located on that card, to the "Test" position. This action briefly rendered this loop of the containment pressure system inoperable, and generated a containment pressure loop alarm. The technician immediately identified and corrected the problem. The plant's problems and failure modes analysis concluded that the technician had operated the test switches on the wrong card frame because he had become "spatially misoriented." It further stated that he had failed to follow the common practice of locating the card that was to be manipulated, and then verifying the card's location via a secondary means, such as the identification sticker on its back.

In the second incident, maintenance personnel performing a surveillance discovered that the coarse setpoint dial for the RCS wide-range pressure loop was incorrectly set at 5 instead of 0. The dial was located on a bistable circuit card in card slot B2-246. In the adjacent slot, B2-245, was a lead/lag card for a steam generator pressure loop. It had a coarse time dial that looked the same as the dial on the bistable card, and both were located at the same height. About two weeks earlier, the lead/lag card had been serviced, using a procedure that required its dial to be reset to a value of 5. The plant's evaluation concluded that when the technicians intended to reset the dial on the lead/lag card to "5," they had incorrectly set the dial on the bistable card instead, which rendered a main control board annunciator inoperable.

The following are three possible explanations of how these incidents occurred. Each explanation leads to corrective actions that are somewhat different.

The first explanation is that the error occurred from a mistake in identifying the card. The technician might have misread the description of the card's location in the maintenance instructions, or misread the label on the circuit card, and consequently, identified the wrong card. This may be considered a mistake (i.e., an incorrect plan or intention) because the technician performed all of his actions as planned. However, the plan was flawed because the wrong card had been selected, based on inadequate use of available information. (This error is similar to the incident described by the second bullet, in which the technician identified the correct component but misread its required setting.) This type of error may be addressed by measures that aid in correctly identifying the card (or setting) and

may include ensuring that the card's identification numbers are legible in the maintenance instruction (e.g., the type is highly legible), making the card's identification labels more visible, and training the maintenance personnel to verify the correct location of the card.

The second explanation was that the context of the task caused the technician to access the wrong card. In the first incident report, the technician was required to work with card frame 2 and then with a card that had a similar number but was located on a different frame (frame 4). If the maintenance instructions did not make clear that the switch was located on a different card frame, the technician might have expected it to be on the same one, so contributing to his failure to detect the slight difference in card numbers (B4-235 versus B4-435). This error may be rectified through the design of the maintenance instructions. For example, they could explain more clearly that a transition to a different card frame was necessary (e.g., "Moving to card frame 4 ..."). Other approaches may include highlighting the differences between cards B4-235 and B4-435 (e.g., color coding) and training personnel to verify the correct location of the card.

A third explanation is that the technician identified the correct component but reached for the wrong one. This is an example of a type of slip called a description error (Stubler, O'Hara, and Kramer, 2000). It occurs because the correct response is not adequately "described" by the design of the user interface. That is, the user has the correct intention but the execution gets waylaid by an ambiguous user interface. Description errors may occur when similar looking options are in close proximity. In this case, the consistency of the user interface (i.e., the use of the same switches and dials) contributes to the likelihood of this slip because adjacent interfaces look similar and are similarly operated. The likelihood of this error might be lessened by making the circuit boards, dials, and switches more visually distinct, by using color coding or prominent labels. In addition, these errors may be detected by verifying the action (e.g., a supervisor could inspect the completed work to determine that the correct switch or dial was properly set). The practice of verifying the location of the component *before acting*, as discussed in the first incident description, is not likely to reduce this error. The slip was assumed to occur *after* the technician initially identified the correct component. Whatever the actual cause, the likelihood of each of these types of errors may be reduced by independent verification of maintenance actions that are important to risk.

The second bullet describes an incorrect trip setting for a motor-operated valve coil, which occurred because the maintenance technician read the work order incorrectly. This incident is an example of a random, unintended action that can be overcome by personnel training.

The third bullet describes an incident in which the maintenance technicians were unaware that the components they were servicing belonged to different loops or channels; it stemmed from inadequacies in the work order, which identified the numbers of the components but not the loops to which they belonged. The technicians assumed that they all belonged to the same channel, which had been taken out of service. Because this was not the case, their actions tripped a second loop. Consequently, two out of four channels were out of service, which triggered the alarm and the movement of the valves.

The fourth bullet describes an incident that resulted from an incorrect wiring diagram. Because the diagram was faulty, the annunciator was not wired properly and, consequently, was inoperable. Such incidents may be addressed by reviews verifying maintenance interfaces and their supporting documentation.

The incidents in the fifth and sixth bullets are random, unintended actions that can be corrected by personnel training.

Maintenance errors resulting in servicing the wrong digital component are likely to increase as NPPs install more digital systems, thereby creating more opportunities for maintenance workers to make such slips. Further, the complexity of digital systems (see Section 4) may make detecting errors more troublesome. Before more definitive review guidance can be developed, we need to develop a better understanding of the types of errors that occur when

the wrong component is serviced, and the contributory factors. More reviews and research are needed, including further reviews of event reports and interviews with subject matter experts.

5.2.3 International Studies of Digital System Failures

5.2.3.1 Digital System Failures in Canadian NPPs

Operating experience with computer-based control, monitoring, and safety systems in Canadian nuclear reactors was reviewed to investigate safety issues (Arsenault, Manship, and Roger, 1996; cited in Ragheb, see Footnote 1). This review was based on information from analyses and reviews by the Canadian Atomic Energy Control Board for Canadian reactors. It addressed 459 significant-event reports from 22 reactor units over 13 years (1982 through 1994).

Ragheb reported the following preliminary findings from the Arsenault et al. study:

- Failures attributable to inappropriate human actions have shown an increasing trend in the last 5 years; overall, they accounted for about 25% of the events involving computer-based systems. (Most other trends, such as failures due to computer hardware, software, ancillary equipment and connections, and power supply faults, were either decreasing or flat.)

- Software faults continually decreased indicating that latent faults remaining from development were gradually corrected. Software problems are sometimes fixed by temporary changes (patches) installed outside the programmable part of the software. These patches can cause further problems, even when installed properly. For example, in one event, a patch was installed to force software to operate correctly at very low reactor power levels (i.e., some irrational power-sensor values occur during reactor startup). However, the patch was not removed when the reactor's power was increased. Consequently, the "patched" plant software operated incorrectly and caused a power excursion, which was terminated by a reactor trip. This particular event indicated the importance of developing and adhering to procedures for modifying software.

- The trend for computer-system failures due to hardware failures is decreasing. A leading cause of hardware failures has been the failure of ancillary devices, such as sensors and relays. This finding led to the conclusion that hardware failures should be assessed in terms of their effect on the performance of system software, as well as the loss of hardware availability. The second highest category of hardware failures was failures of circuit card assemblies, connections, and peripherals. Several incidents were associated with programmable logic controllers (PLCs) installed as cost-effective replacements of older analog or digital controls. These were apparently due to a failure of designers or installers to scrutinize and control the hardware and software of PLCs as closely as the plant's larger computer-based systems.

Ragheb concluded that maintainers need to fully understand software before they change it. After a software change, formal testing with stringent standards should be performed. Inadequately designed or executed tests can fail to reveal software errors. Ragheb states that adequate attention often was not given to the testing tools and facilities used in upgrading computer systems. Also, adequate documentation is essential to reliably modify and test software. Requirements specifying what the software is functionally required to do are the basis for designing thorough tests. Test procedures should give step-by-step instructions, including expected system responses for each step.

5.2.3.2 Fault-Tolerant Digital Control Systems

Paula et al. (1993) studied 20 fault-tolerant digital systems from various process control industries including NPPs from the United States and Canada. Fault-tolerant digital control systems have redundant processors that use

diagnostic routines to detect single faults and isolate the failed equipment. This ensures that the equipment that is still operational takes over the control function. In this study, "system failure" was defined as a failure of the digital control system that leads to a process upset serious enough to shut down the process.

The 20 systems had operating histories ranging from 0.5 to 45 system-years. System-years were determined by multiplying the number of years that the system had operated by the number of systems of a particular type. Four of the digital systems, with operating experience ranging from 1 to 14 system-years, had not yet failed. Thirty-nine failures were identified, eleven of which had unidentified causes. The remaining 28 failures were attributed to 6 causes. The following describes the categories, and indicates the frequency and percentage of failures:

- Software Failures – All software deficiencies that could or did disable the entire system (9 failures; 32%)
- Inadvertent Human Actions – All inadvertent human actions that disabled the entire system (9 failures; 32%)
- Electrical Power Supply – Complete loss of power (e.g., an electrical short within the power supplies) to the processors or input/output modules, or disturbances in the power supply that upset the entire system (5 failures; 17%)
- Spurious Signal Initiated within the Digital Control System – All spurious signals initiated within the digital control system that disabled the entire system (3 failures; 11%)
- Hardware Common-Cause Failures – All hardware deficiencies in redundant equipment that disabled the entire system (1 failure; 4%)
- External Physical Damage – Physical damage to digital control equipment from a variety of external events such as fires, high temperatures, spurious activation of a fire-suppression system (e.g., sprinkler), and physical damage to the input and output cabling (e.g., cutting) connecting the control system to sensors and actuators (1 failure; 4%)

These results were similar to the findings of the NRC reviews described earlier, which named software errors and human actions as the leading causes of failures. Paula et al. (1993, p. 284) gave the following examples of inadvertent human actions, all at Canadian NPPs:

- "During troubleshooting and repair of a data link problem, maintenance personnel caused both computers to fail."
- "While attempting to isolate one failed computer for repair, maintenance personnel removed the wrong computer from service."
- "After changing the computer software on one machine, personnel changed the software on the second machine without waiting 30 minutes as required (i.e., they loaded the second machine too soon)."

Some of the failure events that were not included in the Inadvertent Human Action category also may have been partly due to the performance of maintenance personnel. For example, it may have contributed to the following failures identified in the Spurious Signal category, which occurred during maintenance in U.S. NPPs:

- "The trip occurred on Unit 2 when a configuration and tuning module was being plugged into a controller bin. During insertion, noise generated a spurious (erroneous) signal that caused one of the feedwater valves to open fully, resulting in a reactor trip" (Paula et al., 1993, p. 281).

- "During testing and maintenance of computer and control circuitry for operating switchyard power circuit breakers, a spurious signal was generated that caused a number of 230 kilovolt breakers to open. This caused a chain of events that ultimately disconnected both main unit transformers from the grid and tripped Unit 1" (Paula et al., 1993, p. 282).

- "This event occurred during troubleshooting related to the loss of all off-site power event four days earlier. When a card was removed from the breaker control multiplexing multiprocessor, the same breakers opened that opened during the [previous] event, resulting again in loss of all off-site power" (Paula et al., 1993, p. 282).

Paula et al. observe that an important difference in the reliability of digital systems exists between control functions of different complexities. Systems in simpler applications perform more reliably than systems in more complex applications.

Paula et al. conclude that while fault-tolerant digital control systems can, in theory, be highly reliable, the levels of reliability achieved in practice are much smaller. "Even the more modest goals can only be achieved with great effort at the design stage (particularly, software design) and with excellence in operation/maintenance throughout the life of the system" (Paula et al., 1993, p. 273). They believe that most failures of fault-tolerant, digital control systems can be traced to some kind of common-cause failure, such as software failures and inadvertent personnel actions; the latter were identified as a leading cause of failures of fault-tolerant digital systems.

Paula et al. state that the ultimate defense against process failures is to provide diversity in the designs of both the hardware and software of digital systems. However, as a practical alternative to this expensive approach, they recommend designing digital systems for ease of maintenance, training personnel well, and implementing good maintenance practices. For good training and maintenance practices, they recommend the following:

- Provide clearly written manuals and maintenance procedures

- Use simulation-based training for maintenance personnel on inserting/pulling printed circuit cards; switching processor, modules, and power supplies; bypassing subsystems; and isolating communication buses

- Use the same teams of design and installation personnel for each digital system, so that new installations can benefit from their previous experience.

5.2.3.3 Programmable Logic Controllers (PLCs)

A PLC is a digital controller that uses a microprocessor to process signals. They have been used as low-cost replacements for older analog and digital equipment. Paula (1993) studied the failure rates of PLCs used in foreign NPPs and a chemical plant in the United States. He found their failure rates to be very consistent (within a factor of 3) and much lower than those of larger digital systems. For example, fault-tolerant digital control systems, such as those used in safety-related control, monitoring, and protection systems in Canadian NPPs, had failure rates that were 15 to 50 times higher than those of PLCs. Mitchell and Williams (1993) also reviewed the failure rate of PLCs used in the emergency shutdown systems of natural-gas compression stations. Here, a major source of failures of PLCs was human errors during testing and maintenance carried out in the cabinets of these devices, such as inadvertently causing shorts on electrical leads. However, specific failure rates due to human error were not given.

5.2.4 Conclusions from Reviews of Industry Experience

The reviews of industry experience with digital systems were from many domains, although experiences in U.S. and Canadian NPPs featured prominently in the events cited by these reviews. Due to the overlapping scopes of these reviews, some events appeared in more than one. A leading cause of digital-equipment failures was software errors

introduced during the development process. Once digital equipment is put into service, it is highly susceptible to faults caused by human actions during tests and maintenance. Some conclusions may be drawn from these reviews about the demands imposed on personnel in maintaining digital systems. In particular, the unique characteristics of digital systems make them more susceptible to mistakes (errors of intention) and slips (errors of execution) during maintenance.

For mistakes, it was found that computer-based processors, key features of digital systems, add a degree of complexity that may not have existed in earlier I&C systems (Lee, 1994). Knowing how a unit of digital equipment works and how it interacts with other digital equipment requires an understanding of the structure and operation of software. Several different types of mistakes were identified, including failure to consider the consequences of loading uncontrolled versions of software, attempting to clear alarms by rebooting a processor, taking unsuitable actions because of a lack of awareness of which redundant processor is in control, and performing improperly due to a failure to recognize mismatches between primary and backup processors when transferring control between them. For slips, the events discussed in these reviews indicate that digital equipment can be highly susceptible to faults caused by people's unintended actions during tests and maintenance. These include failure to follow steps properly when rebooting a processor, mode errors (e.g., failure to recognize the current system mode), keying errors, and connecting test equipment to the wrong port or system.

Both design-oriented and process-oriented strategies can reduce the likelihood and consequences of maintenance errors. Design-oriented solutions include designing digital systems for ease of maintenance, as suggested by Paula et al. (1993). Cognitive demands related to mistakes may be resolved by reducing the complexity of digital equipment; for example, making it more modular, and labeling components and connections may allow maintenance personnel to better understand the functions and relationships of subsystems, modules, and parts. Slips may be overcome by designs that draw attention to incorrect actions or make them difficult to complete. For example, labeling may support correct identification of components (e.g., circuit board A) and actions (e.g., turn power On-Off), parts may have physical characteristics that prevent errors in assembly (e.g., components can only be installed in the correct orientation in the correct connector or fixture). (Section 9 contains many guidelines that address these strategies.)

Process-oriented solutions also address the planning and execution of maintenance tasks. NRC Information Notice 96-56 (NRC, 1996) stressed the need for proper planning and control of maintenance while the plant is at power. Paula et al. (1993) added other suggestions, such as providing clearly written manuals and maintenance procedures and simulation-based maintenance training, and using teams to capitalize on expertise in design and installation.

5.3 Interviews with Subject Matter Experts

As described in Section 3.3, on-site and telephone interviews were conducted with experts familiar with maintenance issues for the following domains: nuclear power, fossil power, commercial aviation, military aviation, and aerospace. Below are some key points identified through the interviews.

5.3.1 Foreign Nuclear Power Plants and Domestic Coal-Fired Power Plants

Many coal-fired power plants have distributed digital control systems that make extensive use of continuous, automatic test features. Digital components are constantly tested for faults and alarms are automatically generated when they are detected. Also, the time and nature of the detected fault may be automatically logged. These features greatly aid the detection, diagnosis, and correction of malfunctions.

Discussions with personnel from coal-fired plants identified problems with on-line maintenance similar to those identified in the reviews of industry experience. Digital control systems that feature redundant processors allow maintenance to be performed on one processor while the other is controlling the plant system. The processor that is

out of service may be replaced, adjusted, or have new software installed. After the work is completed, control may be restored to the modified processor. Then, the other redundant processor(s) may be similarly serviced. One problem is that a high degree of operator skill may be required to restore control capability to the serviced processor. Before switching control from one controller to another, the control signals of the two processors must be matched. If the difference between the signals is great, the plant system is sent a signal instructing a large change over a short time. The plant system may not be able to respond properly, and a "bump" is said to occur. In many control systems but not in all, this matching is performed automatically. Also, this function may not be automatic in some modes, such as manual control and test modes. Plant personnel may fail to recognize that a mismatch exists and that a transfer may upset the system. Interviewees indicated that system upsets caused by errors in switching between processors during on-line maintenance are not infrequent.

These examples indicate that on-line maintenance can impose special demands on the ability of personnel to understand how the control system is configured and anticipate how it will react to a change in that configuration. Changes in configuration may include switching the control capability between redundant processors and switching controllers between the various operating and test modes. On-line maintenance for NPPs should be seriously considered during HFE reviews. Errors committed during on-line maintenance can have consequences just as serious as those committed during plant operations; both can disrupt operations and initiate transients. Review activities, such as human factors verification and validation, should ensure that on-line maintenance capabilities operate as intended, and can be used effectively by plant personnel.

Interviews with personnel from a NPP also indicated problems with ATE. One utility, which used a portable, handheld automated test device, found that maintenance technicians were confused by the many screens and test capabilities provided through the menu-driven interface. To alleviate this problem, engineers modified the manufacturer’s standard menu structure. They developed a smaller one which by-passed capabilities that were not used by the maintenance technicians, and they added a figure depicting the menu structure and its navigation paths. They stated that the resulting ATE was easier to use.

5.3.2 Aerospace Systems

The aerospace industry has a longer history of using digital technologies, such as built-in and automated test capabilities, than U.S. NPPs. In some respects, maintenance considerations for aerospace systems are similar to those of NPPs. Aerospace systems are designed so that maintenance can be carried out while the system is in operation, as are NPP systems; this is especially true of a vehicle intended for long-term missions, such as the Space Station – in contrast with commercial and military aircraft for which maintenance usually is performed on the ground.

A major concern for aerospace systems is the need to address preventive and corrective maintenance early in the design process, including systematically analyzing the expected failure rates of equipment to determine which type of maintenance will be necessary, and its expected frequency. This leads to considerations of the (1) location of equipment to access, (2) access to any internal components, (3) failure indications and test equipment needed to detect and isolate equipment failures, (4) equipment design features, tools, and facilities needed for maintenance, and (5) logistical considerations somewhat unique to space vehicles. As an example of maintenance facilities, an on-board workstation was designed for Space Station Freedom and the subsequent International Space Station to support maintenance that may have to be performed while the station is in use.

The following are some specific considerations associated with aerospace systems. Similar ones exist for NPPs.

Equipment Accessibility - Often, equipment that is functioning properly must be removed to access failed equipment. This increases the amount of time needed to perform the maintenance task, and increases the likelihood of damaging the equipment which was operating properly.

Component Accessibility - Hardware components may be embedded in larger units of equipment. The accessibility of all components must be considered during the design process.

Accessibility of Replaceable and Consumable Items - Replaceable and consumable items are sometimes difficult to access, remove, and replace (e.g., the many electrical fans used to cool equipment on a space vehicle). Typically, each piece of equipment has its own ventilation fan, equipped with an air filter. Once the piece of equipment is accessed, multiple screws and covers may have to be removed to get to and replace the air filter. Maintainability may be improved by reducing the number of such screws and covers.

Preventive Maintenance - Inadequate attention is often given to the requirements for preventive maintenance, such as accessibility and ease-of-use of test points, service points, and serviceable items.

Tools - When many different tools are required, higher demands are placed on personnel for storing, finding, transporting, and using them. A goal is to reduce the number and types of needed tools. For example, a systematic review of fasteners may reduce the types of screws used across the equipment, thus reducing the number of screwdrivers needed.

Logistics - Logistics and resupply for parts, tools, and replacement hardware is a carefully studied, planned activity for a space vehicle because it is difficult to obtain them once the vehicle is in space. Commonality of hardware equipment design can increase the degree to which components may be interchanged and reduce the variety of tools required on a flight.

To address Space Human Factors issues, NASA developed NASA-STD-3000 (NASA, 1987) and most recently, NASA-STD-3000B (NASA, 1995). Section 12, Design for Maintainability, of NASA (1995) was written specifically to address maintenance topics, and describes HFE principles for ensuring maintainability in aerospace systems.

5.3.3 Commercial and Military Aviation

Discussions with experts on maintenance of commercial and military aircraft identified similarities and differences between the nuclear and aviation domains. Both types of aircraft feature digital technology prominently in their control and monitoring systems, and use built-in and automated test capabilities extensively. These systems can monitor system performance while the aircraft is in flight and indicate failures when they occur. Also, they can automatically maintain records of key system parameters and the occurrence of failure indications. Maintenance is rarely performed on-line (i.e., while the aircraft is in flight).

To reduce the amount of time required to return an aircraft to service, designers have greatly modularized aircraft design. Aircraft systems are composed of line-replaceable units, which often take the form of boxes with electrical and mechanical connectors. For example, an altimeter may consist of a single, line-replaceable unit inside which may be printed circuit boards and smaller components. This modularization has made a sharp distinction between the type of maintenance performed at the aircraft and in the maintenance depot (maintenance shop).

Maintenance personnel who work on the aircraft typically are responsible for diagnostic testing, identifying line-replaceable units that appear to be the source of the failure indication, replacing faulty line-replaceable units, and then returning the aircraft to service. Experts from both commercial and military aviation indicated that the decision-making process used by these maintenance personnel for unscheduled maintenance is largely rule based. Many of the tests and evaluation criteria are predefined.

Automatic tests are used to evaluate many functions of aircraft systems. Maintainers attach the test equipment, start the test, and then read the fault codes generated. Fault codes can be interpreted by looking up the specific code on a

table presented in paper- or computer-based form; errors may occur during each of these stages. For example, maintainers may make errors when reading the fault code from the test equipment or interpreting its meaning from the table. The maintainer may look at a table for interpreting code "111," but, instead, read the interpretation for code "112." When routine tests are inadequate, maintenance personnel must use special knowledge of the aircraft to develop and test hypotheses about possible faults. Maintenance personnel sometimes can access additional information stored in an aircraft subsystem or the aircraft's central maintenance computer to aid in diagnoses; this may be a chronological record of failure indications and operating conditions that were experienced before and during the failure. By comparing the historical information with current data, they may be able to better identify the failed line-replaceable unit.

Maintenance personnel who work at the depot are typically responsible for repairing equipment. For example, they may disassemble a line-replaceable unit, identify and replace faulty printed circuit boards and other components, reassemble the unit, and then test it to ensure that it is working properly. Such personnel often have specialized skills. An individual may be specially trained to test and repair the line-replaceable units of a particular system, such as the inertial navigation system. Troubleshooting may require more extensive diagnostic skills and access to historical information about failure indications and operating conditions.

In the past, printed circuit boards were repaired at the depot by replacing individual components. However, new manufacturing processes for circuit boards make it difficult or impossible to do this. Now, failed circuit boards are usually discarded. (Note that printed circuit boards and other small components usually are not replaced at the aircraft because the work environment often is not suitable for handling them.)

Software design is tightly regulated by the FAA. Vendors rather than airline personnel usually install software to upgrade a software-based system.

Usually, maintenance personnel located at the aircraft can rapidly perform automated diagnostic tests, trace the fault codes to line-replaceable units, and replace them. Consequently, replacing these units has not been as much of a safety concern as other maintenance tasks, such as inspecting aging aircraft for structural faults, and maintaining mechanical components.

A major concern with digital maintenance is the frequency with which ATE results obtained at the aircraft cannot be subsequently duplicated in the maintenance depot. If personnel in the depot cannot obtain the same result for a line-replaceable unit as was obtained at the aircraft, then it may be hard to determine whether the original result was due to an intermittent failure, an incorrectly performed test, or an error in reading or interpreting the results. Between 30 to 60 percent of line-replaceable units removed from aircraft and sent to maintenance depots for repair are eventually labeled "cannot duplicate," meaning that subsequent tests do not indicate a problem with them (Maddox, 1996). These units cannot be reinstalled in an aircraft unless it can be shown that they are not defective. Thus, a high "cannot duplicate" rate has serious economic implications, and may indirectly affect safety. If 50 percent of the line-replaceable units sent to a depot are eventually labeled "cannot duplicate," then approximately one-half of the maintainers' time may be spent on equipment that, ultimately, will not be fixed. This can greatly reduce an organization's capacity, in terms of personnel, equipment, and time, to properly diagnose and repair other failed equipment (Maddox, 1996).

In addition to unscheduled maintenance, aircraft also are subject to periodic inspection and maintenance requirements mandated by federal regulators. These scheduled inspections are similar to maintenance outages in NPPs; extensive inspecting and testing must be done before the aircraft can be returned to service.

There are important differences in the design and maintenance of digital systems between the nuclear power and aviation industries, some of which are highlighted below.

Division of Maintenance Labor – As with the aviation industry, NPPs often have separate groups of maintenance personnel for working locally in the plant, and in the maintenance shops. However, the roles of these groups are somewhat different. Many aircraft components are designed as modular, line-replaceable units, and the role of the local maintenance personnel is to remove them and transport them to the maintenance depots, where shop personnel carry out the more demanding tasks, such as removing and replacing circuit boards. In NPPs, many of the demanding tasks, such as replacing circuit boards, are performed by local maintenance personnel (i.e., at the local electrical panel).

Modularization of Digital Equipment – The digital systems of NPPs often are not as extensively modularized as in aircraft. For example, digital systems in NPPs usually consist of cabinets, located locally in the plant, containing racks of printed circuit boards and other components. Individual boards in these cabinets may be removed and replaced. Mitchell and Williams (1993) identified errors associated with maintenance activities performed in local equipment cabinets as a major source of failures of PLCs in NPPs. By contrast, digital systems in aircraft are usually composed of line-replaceable units – boxes that can be rapidly removed and replaced.

Point-To-Point Wiring – Digital systems installed in existing NPPs as replacements for older analog or digital equipment are usually connected by electrical wires or cables. Data-bus architectures, which transmit signals for multiple components through the same wire or conduit, have been proposed for future reactors but are not widely used in existing ones. By contrast, data buses are currently used in aircraft. There is a trend toward increased use of data buses in NPPs, using communication technologies such as optical fibers; however, this may result in some types of errors that do not occur when point-to-point wiring is used. With point-to-point wiring, connections can be checked by electrical tests. With a data bus, connections are made by assigning network addresses to components that communicate with each other. These addresses might have input errors, such as omitted or transposed numbers and letters, and detecting them through inspection also may be error prone.

On-Line Maintenance – Testing and replacing components and installing software may be performed while a NPP is operating. System "bumps" and plant trips may be experienced when maintenance personnel take a processor out of service or switch control between redundant processors. Such maintenance is not usually performed while an aircraft is flying; thus, aircraft do not experience the functional equivalent of a plant trip due to maintenance.

Installation of Software – Software for digital systems may be installed by NPP maintenance personnel or vendors. In aviation, vendors almost always do this.

5.3.4 Conclusions from Interviews

Many similarities and some significant differences were noted in the maintenance practices of the domains represented by these interviews. Commercial aviation, military aviation, aerospace, and coal-fired power plants have used digital equipment in their systems for many years. By contrast, the nuclear power industry has limited experience with digital systems.

All of these industries used built-in, automatic test capabilities to some extent. Coal-fired plants that have integrated digital control systems rely heavily on continuous, automatic test features to generate alarms and log entries when malfunctions are detected in the computer's hardware. In commercial and military aircraft, built-in ATE is used extensively to isolate faults. This equipment automatically tests systems and identifies line-replaceable units that are likely to contain a fault. Results are often presented as coded messages, which maintenance personnel must interpret. However, errors may occur when they misread the codes or use the look-up tables incorrectly. Automatic logging capabilities provide historical records of malfunctions and the operating conditions that occurred before, during, and after the malfunctions. This information can be very useful for diagnosing the cause of failures. A major economic concern for the aviation industry is the high rate at which initial tests suggest that a component should be replaced, but subsequent tests fail to find a fault.

The digital systems of NPPs, coal-fired power plants, and aerospace systems have been designed to enhance availability by supporting on-line maintenance. However, on-line maintenance can impose special demands on personnel. Errors include taking the wrong processors out of service and failing to match the signals of processors to avoid a "bump" when transferring control capabilities between processors. These errors can activate protective features (e.g., plant trips).

One problem of particular concern in the aerospace industry is the failure to adequately address requirements for maintainability during the design process. Many problems experienced by the aerospace industry are similar to those experienced in NPPs: inadequate access to equipment, internal parts, and consumable items; inadequate planning for preventive maintenance; inadequate planning for tools (e.g., special tools needed, and lack of coordination of tool requirements across equipment); and, inadequate planning of logistic requirements.

One difference between NPPs and aircraft is the way their digital systems are packaged and maintained. In NPPs, maintenance, such as diagnostic tests and replacement of circuit boards, often is carried out at electrical cabinets located throughout the plant. In commercial and military aircraft, digital systems are designed as a series of box-like, line-replaceable units that can be quickly removed and replaced to restore the aircraft to service. This results in a sharp division between the maintenance tasks performed at the aircraft and those undertaken in the maintenance depot. Maintenance personnel who work at the aircraft are skilled in diagnostic testing to identify and then remove and replace faulty line-replaceable units. They often rely on the results of ATE and heuristics to identify faulty equipment. Personnel at the maintenance depot repair the line-replaceable units, and often have specialized expertise for particular units. Their diagnostic tasks may require a great degree of knowledge-based reasoning for generating and testing hypotheses. In NPPs and coal-fired power plants, there is a not as clear a distinction between the types of maintenance tasks performed in the field and in the maintenance shop, but as the use of digital systems increases in NPPs, there may be a trend toward greater specialization. This may raise concerns about coordinating information and expertise among maintenance personnel.

Another difference between digital systems in NPPs and aircraft is the use of data-bus technology. There is a trend in commercial and military aircraft design to use data buses connecting components via addresses rather than using point-to-point wiring. This introduces new opportunities for maintenance errors. For example, a sensor may send signals to the wrong processor if there is a typing error in its address. This may become a growing concern in NPPs as more complex digital systems are installed.

5.4 Human Performance Considerations Identified from Literature

The following describes human performance considerations identified by reviewing literature related to maintenance; they are troubleshooting, accessing digital components, and using test equipment.

5.4.1 Troubleshooting

While troubleshooting always has been one of the most demanding tasks for maintenance technicians, it is becoming more complex for large systems, such as process plants and aircraft. Further, to improve their performance, efficiency, and safety, the design of these systems is becoming increasingly complex. As a result, the troubleshooter is forced to deal with increasingly complicated situations that occur infrequently due to this increased reliability (Johnson and Rouse, 1982). The long interval between failures makes it more difficult for troubleshooters to draw on relevant, recent experience. For complex equipment, most corrective maintenance time is spent on isolating faults – trying to identify the unit of equipment causing a malfunction (Majoros and Boyle, 1997). The strategies for isolating faults in digital systems differ from those used in analog I&C systems. For analog I&C equipment, individual components can be inspected and tested more directly. Failed components may be detected by observing loose or charred connections, smelling burnt components, or taking electrical measurements across suspicious components. For digital I&C equipment, maintenance personnel must often resort to less direct, symptomatic

strategies, in which performance-based symptoms identified at a functional level must be related to individual modules, printed circuit boards, integrated circuits, and simple circuits. As a result, finding faults in digital equipment can impose more cognitive demands than doing so in analog equipment (Klauer et al., 1993). While the introduction of fault-tolerant systems and ATE has helped to some extent, adding such features can also *increase* the system's complexity. In addition, when fault-tolerant systems and ATE cannot handle a problem, personnel may be faced with an extremely complex troubleshooting task (Johnson and Rouse, 1982).

There has been extensive research on troubleshooting and related human problem-solving behavior. Over the past 15 years, studies have included skills training, problem-solving strategies, cognitive styles, behavioral and organizational characteristics, problem-solving models, and task variables affecting troubleshooting (Teague and Allen, 1997). One conclusion drawn from this research is that humans are not optimal troubleshooters (Henneman and Rouse, 1984; Kahneman et al., 1982; Rouse and Rouse, 1982; all cited in Teague and Allen, 1997). Personnel find it easier to incorporate some types of data into their decision-making processes than others. For example, it is easier to use test results that indicate that a component *is not* working properly than to use ones showing that it *is* working properly.

Troubleshooters typically test portions of a malfunctioning system and then integrate this information to develop hypotheses about the system's state that form a basis for subsequent tests and hypotheses (Teague and Allen, 1997). Troubleshooting may begin by analyzing initial system outputs, such as instrument readings and the state of the system, to identify the possible causes of the malfunction. The set of possible failures consistent with the given symptoms is called the consistent fault set (CFS) (Duncan and Gray, 1975; cited in Toms and Patrick, 1989). Two types of strategies used for identifying the CFS are symptomatic and topographic (Rasmussen, 1981, 1984; cited in Toms and Patrick, 1989). In symptomatic strategies, possible failures that correspond to the symptoms are accessed by searching a "library" of abnormal system state patterns. The library may take the form of familiar system states stored in a person's long-term memory, or may reside in external decision tables (Toms and Patrick, 1989). An advantage of symptomatic strategies is that they efficiently use information and prior experience. For example, using a symptomatic strategy it may be possible to move directly from a particular symptom to an exact specification of the failure. However, instructing a troubleshooter in a symptomatic strategy may have disadvantages. It is "...liable to be demanding on memory, inflexible, and inadequate in situations in which individuals are required to deal with previously unencountered fault-symptom combinations" (Toms and Patrick, 1989, p. 466). In topographic strategies, possible failures are inferred from the basis of the system's structure. The fault-finder, in essence, performs a "...good/bad mapping of the system through which the extent of the potentially bad field is gradually narrowed until the location of the change is determined with sufficient resolution to allow selection of an appropriate action" (Rasmussen, 1984; cited in Toms and Patrick, 1989, p. 466).

Toms and Patrick (1987) studied topographic strategies in troubleshooting in simulated networks and identified two components of the fault-finding process – symptom interpretation and search. Symptom interpretation addresses the identification of network components that might be faulty. Search addresses the selection of tests to discriminate between possibilities to obtain further information about the fault's location. Theoretically, the most efficient test that a fault-finder can perform is a split-half test. This test eliminates one-half of the items from the CFS and, thus, provides maximum information about the location of the fault in the fault set (Maddox, 1996). The symptom interpretation and search components of fault-finding are iterative; which occurs first depends upon the particular task. The tasks investigated by Toms and Patrick were (1) identifying the set of possible faults (the CFS), (2) applying the split-half rule to a specified CFS, and (3) making the first test without specifying the CFS. Network size and complexity (as defined by four types of CFS configurations) were manipulated. Their study found that symptom interpretation and search were not correlated and had different sources of degradation. Subjects found it more difficult to identify the CFS than to correctly apply the split-half rule to the specified CFS. Errors that occurred when identifying the CFS (symptom interpretation) were mostly omission errors (identifying the CFS to be smaller than its actual size). At the initial phase of the fault-finding task, subjects were more likely to underutilize positive information (e.g., indications of faults), thereby omitting items from the CFS, rather than including ones that

were not actually in the CFS. This effect was exacerbated in larger networks. Symptom interpretation was degraded by increasing the network size and the complexity of the CFS. The same pattern of effects was observed in selecting the first test when the CFS was not specified. The ability to select a split-half test from a given CFS was affected by the complexity of the CFS configuration; that is, network size affected only identification of the CFS.

In a subsequent study, Toms and Patrick (1989) examined two alternative strategies, elimination and direct back-tracing, that may be used by troubleshooters in the symptom-interpretation phase of a topographic search of a malfunctioning system. In the eliminative strategy, all components of the malfunctioning system are initially considered and then components that could not possibly be faulty are eliminated from further consideration. In the direct trace-back strategy, the troubleshooter traces back from bad system outputs to a set of possible failures. Because a purely eliminative strategy requires consideration of all components in the system, it is more thorough and demanding of troubleshooters' processing resources than the direct trace-back strategy. Using the eliminative strategy without the support of an external aid, such as a computer, may overload the short-term or working memory of the troubleshooter. By contrast, the direct trace-back strategy, which requires considering only a subset of components (those feeding the bad outputs), is less demanding of memory. Computer aids were developed to support both strategies by tracking the components and test results.

Forty-eight troubleshooters were presented with forty network problems, representing four different types of CFS structures. To examine verbal versus visuospatial demands associated with the elimination and direct back-tracing strategies, each troubleshooter was assigned to one of three categories of memory loading, as defined by the type of memory aid permitted. These categories were as follows: (1) a diagram incorporating visuospatial information, such as the identity of, location of, and relationships between, CFS units, which the troubleshooter could mark, (2) a listing of units by number (e.g., a verbal listing of all possible failures and a troubleshooter-generated listing of components that were not considered possible failures), and (3) no aids.

It was found that the eliminative strategy improved the accuracy of symptom interpretation slightly when supported by a visual memory aid, but depressed accuracy when combined with a verbal memory aid. When no memory aid was permitted, troubleshooters apparently were unable to use the eliminative strategy. When troubleshooters used the less demanding direct back-tracing strategy, there was no difference in accuracy between visual and verbal memory aids. It was concluded that the relative efficacy of the two different strategies may be mediated by the memory load associated with them and the level of support provided by external memory aids. When a high degree of external support is provided, using an eliminative strategy for identifying CFS entails fewer errors of omission and may overcome effects of problem complexity. However, with less external support, the eliminative strategy may lead to severe decrements in performance. That is, troubleshooters apparently encountered more difficulty in ruling out failures that could account for some, but not all, of the observed symptoms. The results also suggest that when designing troubleshooting aids or training aids, it is important to consider both the demands imposed by the symptom interpretation strategy and the type of aids available in the fault-finding situation.

Teague and Allen (1997) studied the effects of uncertainty, as caused by intermittent failures, upon troubleshooting behaviors. Intermittency is a factor that troubleshooters regularly encounter. It poses special challenges because troubleshooters must not only consider questions of whether or not a particular component is involved in a fault, but also whether particular results are credible. Intermittent failures require troubleshooters to hold and manipulate more items in memory over longer times than situations in which failures are not intermittent. Intermittency was defined as the rate at which a network component or output, when tested, indicated that it was working when it was not. The troubleshooting task was to find the faulty component that caused a network to malfunction in 18 computer-based problems.

Two problem-solving experiments were conducted. In the first, one-half of the troubleshooters were told whether the problem involved an intermittent failure before the experiment started. In the second, one-half of the troubleshooters were given the specific *rates* of intermittency of the problems before starting. Merely informing the

troubleshooters that the fault was intermittent did not affect troubleshooting performance. However, those given the specific intermittency rates performed better on the troubleshooting problems than those who were not given this information. The results of this study suggest that when troubleshooters have some sense of how often the results of their tests can be believed, they use information more efficiently and minimize unnecessary tests. For example, displays that depict system components and test intermittency rates may be valuable aids for troubleshooting because they may reduce unnecessary and expensive fault-finding tests.

Time pressure is also an important consideration in troubleshooting. The troubleshooting behavior of maintenance personnel is generally oriented toward minimizing the amount of time spent, but is not necessarily systematic nor logical (Majoros and Boyle, 1997). When a unit of equipment is easy to test, maintenance personnel are more likely to invest the effort necessary to identify the specific failed component before beginning to remove components. Features that support testing include well-marked test ports, easy to follow diagnostic logic, and BIT features. However, when testing is more difficult, they are more likely to skip the fault isolation step and instead, begin removing and replacing all suspect modules until the faulty one is found (Majoros and Boyle, 1997). They may undertake the fault-isolation step later to find the failed component in the module, and perhaps to determine its likely cause. However, this strategy of removing and replacing suspect modules and deferring fault isolation has disadvantages; often, subsequent testing is not successful in identifying the failed component (see Section 5.3.3).

5.4.2 Accessing Digital Components

For digital systems to be maintained, personnel must be able to reach components and connect test equipment. The following describes the associated human factors considerations.

Disassembling and Reassembling – It may be necessary to partially disassemble a unit to access internal components for testing, servicing, adjusting, replacing, and repairing. Equipment may be damaged when disassembling and reassembling it. Design features that eliminate the need to take apart equipment for testing include BIT features, and external points for servicing, testing, and adjusting.

Connecting Test Equipment to Test Ports – Errors can occur if equipment is connected to the wrong test ports. Because digital equipment has unique characteristics, labeling is needed to ensure that test equipment is connected properly. For example, channel trip functions were actuated at one plant when a digital voltmeter was plugged into an analog test point of a digital reactor-protection system (Galyean, 1994, Appendix A, p. 4).

Accessing Internal Components – Digital components, such as chips and printed circuit boards, usually can only be tested by ATE via certain access points, such as pins on chips and edge connectors on circuit boards. When these points are difficult to get to, technicians may tend to use other less effective test sequences (Klauer et al., 1993). Bennetts (1984) gives the following recommendations for addressing problems associated with physically accessing and interfacing with the internal components of digital equipment:

- Regular device placement – Two problems associated with using hand-held test probes are their improper placement, and muscular fatigue. These problems may be particularly acute during long test sequences on densely packed printed circuit boards. Tests may not be completed properly if contact with the tested component is broken, or if the test probe accidentally contacts other components. In addition, probes may be mispositioned when technicians move from 14-pin to 16-pin devices. Bennetts suggests that components have a standard orientation (e.g., pin 1 is in the top left-hand corner) to reduce the likelihood of this problem.

- Standard edge connectors – Edge-connector types should be standardized. For example, they should have the same number of connections, and connections for power supplies and ground should always be in the same positions.

- Identification of printed circuit boards – Printed circuit boards should clearly indicate their identification code and modification level.

- Visibility of printed circuit board components – If diagnostic tests are to be performed on a printed circuit board using a hand-held probe, then all components and printed circuit tracking should be visible from a single side of the board. (This may not be possible for multi-layer boards.)

- On-board test points – On-board test points that are not brought out to the edge connector positions should be gathered close together to simplify connecting test leads. They can be grouped by using a dummy integrated-circuit socket or by centralizing the points in a series of connector pins so they can be connected via a socket or plug to the test equipment.

- Space for pin clips – When a component must be accessed via a single-pin or multi-pin clip, there should be space around the component to accommodate the clip.

Removal and Replacement – Removal and replacement of internal components can be facilitated by labeling and modular design. In particular, modules should have sockets or other connectors for easy removal. Their design characteristics should prevent modules from being installed in the wrong orientation (e.g., backwards) and prevent functionally dissimilar components from being interchanged (Wagner et al., 1996).

One strategy used to avoid the fault isolation task is to remove and replace all suspect modules until the faulty one is found (Majoros and Boyle, 1997). Such handling can damage modules, causing loose and bent pins in connectors, for example, which may generate faults. It is desirable to have maintenance personnel remove only the module that contains the fault. Therefore, a basic objective in designing digital equipment should be to allow modules to be tested for faults while in place (Majoros and Boyle, 1997; Bennetts, 1984); this capability should be provided, even if the components are easily removed.

Integrated circuit chips and similar components should be designed with sockets so they can be easily removed for diagnostic tests and readily replaced with new devices. However, where these advantages are outweighed by the risks of damage, such as bent leads during reinsertion, wrong orientation, and replacement with the wrong component, then the components should be soldered into the circuit board (Bennetts, 1984).

5.4.3 Use of Test Equipment

5.4.3.1 General Considerations

Test equipment may simplify the job of the maintainer; reduce the preparation or turn-around time for installing, maintaining, and repairing systems; and reduce total maintenance costs. Accordingly, the test equipment should be fast, easy, and safe to use (Wagner et al., 1996). Simplifying the maintenance job and reducing the turn-around time can return equipment to service earlier, and so contribute to safety by increasing availability. Test equipment can also reduce the likelihood of maintenance errors by reducing the complexity of maintenance tasks and reducing the time pressure associated with their completion.

Decisions about the type of test equipment to be used should be made during the early stages of designing plant systems. Selection should consider the mission, operational characteristics, and anticipated reliability of plant systems. It should also consider the maintenance concept, maintenance staffing, operational environment, the logistics support requirements, and the time and cost of development (Wagner et al., 1996). For example, the mission, operational characteristics, and anticipated reliability of the plant components can determine the degree of precision required for test equipment. Plant components related to safety functions may have strict technical specifications and may require more precise testing than non-safety components. The maintenance concept includes

considering whether plant components should be repaired or replaced. Some digital components, such as printed circuit boards, may not be easily repaired and are simply replaced, instead. Consequently, the test equipment may be required to detect the presence of faults but not isolate them to specific parts on the board.

In the future, the high rate of technical obsolescence of digital equipment may increase the frequency with which plant components are replaced. Staffing considerations for maintenance personnel should include their skills and knowledge as well as their number. In general, test equipment should be selected to reduce the need for highly specialized skills and several personnel to perform a single maintenance task. In addition, the operational environments of NPPs may include spaces with obstructions, high humidity, high or low temperatures, and contaminants or radiation. Test equipment must be compatible with, or resistant to, these environmental factors. In addition, plant equipment located in the maintenance environment may be susceptible to disruption from electromagnetic or other environmental effects. Test equipment should not be affected by these hazards, nor contribute to them (e.g., it should not be a source of electromagnetic interference). Finally, logistics support requirements may include looking at factors such as calibrating the test equipment and transporting it to and from the locations where it will be used.

Test equipment may have some of the following characteristics that limit the ability of personnel to carry out maintenance.

Mode Errors – Mode errors entail performing an operation appropriate for one mode when the system or device is in another mode (Norman, 1983; Lewis and Norman, 1986). They comprise a large class of errors that address many types of human-machine systems, including, computer-based devices. Mode errors occur most frequently in systems and devices with inadequate feedback on their modes or the states.

Factors that may contribute to the proliferation of modes in maintenance equipment are (1) the increased need for information and tests for digital equipment, (2) the increased capabilities of electronic devices, and (3) the need for test equipment to be portable (and, therefore, small). For example, a display screen may show different types of information or a control may regulate more than one variable, depending upon the mode to which it is set. In addition, portable test equipment may be designed to have multiple modes to reduce its size and weight. For example, rather than having a separate control and display for each function, modes can be introduced so the same control and display can be used for multiple functions, thereby reducing the size of the test equipment.

The plant equipment that is to be tested may also have multiple modes, such as manual, automatic, test, and off. In some cases, both the plant equipment and the test equipment must be in particular modes to perform a test correctly. Hence, the proliferation of modes in both can increase the opportunity for errors. For example, if both the plant equipment and test equipment have two modes, then there are four possible combinations. If the test can only be performed with one combination, then it will not generate the correct result in the three others. If feedback is not adequate, the technician may incorrectly conclude that a failed component is operating properly, and plant safety may be compromised by leaving it in service. Conversely, the maintenance technician may incorrectly conclude that a good component has failed. The unnecessary repair work may disrupt or damage other components (e.g., good components may be moved to gain access to the tested component) and, thus, compromise plant safety.

Limited Coverage by the Diagnostic Tool – The diagnostic tool may not address all tests and test conditions needed to evaluate a digital system. Alternatively, the test procedure may detect a fault, but not provide sufficient information to identify the faulty component. Cooke, Maiorana, Myers, Jernigan, and Carlson (1991; cited in Klauer et al., 1993) observed that technicians often encounter the situation in which two or more components are under investigation and no tests are available to identify which component is faulty. Consequently, they may resort to an inefficient strategy of repeatedly replacing and testing components until the problem is eliminated.

5.4.3.2 Automated Test Equipment

The following describes characteristics of ATE that may affect the performance of maintenance personnel.

Mode Errors in Automated Equipment – Most test equipment used in manual troubleshooting only changes modes in response to inputs from the user. However, as ATE and manual test equipment becomes increasingly sophisticated, it may also change in response to situational factors (Stover, 1984; cited in Klauer et al., 1993). Troubleshooting errors may occur because the maintainer is not aware that ATE is in the wrong mode for the type of testing. The interpretation of test results may be greatly affected by the mode of the equipment (i.e., a test indication may have different meanings depending upon the mode of the test equipment). In addition, the need for maintenance technicians to monitor and track the mode changes of the test equipment may impose additional burdens that detract from their primary task of testing and repairing plant equipment. Similar difficulties in maintaining awareness of automatic mode changes have occurred in the operation of computer-based flight-control systems of commercial aircraft. Some automated systems may change modes in response to an operator's action and automatically on reaching a preprogrammed target. Accidents involving aircraft with automated management systems have been traced to the pilot's lack of awareness of the system's operating mode, and to incorrect mental models of how control actions by the pilot or automated system would affect the aircraft. Inadequate feedback from the automated system was an important contributor to these errors (National Research Council, 1997; Sarter and Woods, 1995).

For maintenance of NPPs, the combination of increased automation of modes in test equipment and inadequate feedback to maintenance personnel may result in improperly performed tests that fail to detect damaged components, or result in unnecessary maintenance work, which could affect plant safety. Furthermore, the added burden of monitoring and supervising automated test equipment may affect the quality of maintenance by diverting the technicians' cognitive resources from the diagnosis task to supervision of the automated equipment.

Four design strategies for preventing mode errors include eliminating modes, making modes distinct, requiring different inputs for different modes, and coordinating inputs across modes (Stubler, O'Hara, and Kramer, 2000). The first, eliminating modes, prevents errors by eliminating the conditions under which they occur (i.e., if there are no modes, there can be no mode errors). The second approach, making modes distinct, deals with the problem through feedback. If a salient indication is given of the currently active mode, operators are more likely to be aware of it and less likely to input incompatible data. The third approach, requiring different inputs for different modes, ensures that the same input is not valid in more than one mode. Thus, if the operator provides an input while in the wrong mode, the system will not accept it. The fourth, coordinating inputs across modes, is similar to the third. However, it acknowledges differences in the severity of the consequences of mode errors. Where the consequences do not affect safety, there may be a trade-off between mode errors and the consistency of commands across modes (i.e., the operator's performance may be enhanced by having similar commands in different modes). In such cases, the commands should be designed such that one that produces a benign effect in one mode does not have a severely negative effect in another.

Inflexible Test Sequences – ATE is often designed with the assumption that the users will be novice troubleshooters. However, new users may include experienced troubleshooters, who may not need nor desire a device that leads them step-by-step through a troubleshooting process. These users often have some understanding of the location of a fault and the tests that may identify it further. Troubles can arise when maintenance personnel cannot adjust the preprogrammed tests of an ATE to take advantage of their knowledge or to accommodate special circumstances that occur in the test environment. Some examples include the inability to change the order of tests, adjust their parameters, repeat them, or delay particular ones. For example, inflexible test sequences have required technicians to wait for hours until the ATE program reached the test for the part of the equipment modules suspected of being defective (de Kleer, 1984; cited in Roth, Elias, Mauldin, and Ramage, 1985). Also, this inflexibility may require the repetition of a lengthy series of tests when the technician was only interested in one of them (Klauer et al., 1993).

Providing flexibility is the role of test designers who program the ATE; to do so they must understand the maintainer's knowledge and skills, tasks, and work environment.

Inflexible Interaction Styles – The level of skill of users interacting with the ATE also varies. As they become more proficient, their performance may be slowed by features oriented toward novice users. Flexible interaction styles should be provided to accommodate a range of users, such as by having navigation and help features for novices, and short-cut methods for more experienced users.

Lack of Specific Information for Fault Isolation – The way in which test results are processed and presented can influence troubleshooting performance. One problem with ATE is the ambiguity of information used for isolating faults. For example, the ATE may present the user with a long list of suspect components and little else. The more difficult task of discriminating among possible faults is then left to the technician (Roth et al., 1985).

Insufficient Fault Coverage – Another problem related to the lack of specific information on faults is the inadequate scope of the tests; that is, the set provided by the ATE may not cover all faults that occur in a device. Experience with ATE and other procedure-based aids has shown that while they may be adequate for the vast majority of cases, the most difficult, unanticipated situations may be left to the technician's ingenuity. Thus, attempts to aid troubleshooting via the ATE creates the unfortunate situation in which the technician is forced to deal with the most difficult cases unaided. In addition, the effort required to diagnose these difficult cases may be further increased because the user has not recently made unaided diagnoses of simpler failures (Roth et al., 1985).

Unarticulated Assumptions – Test sequences sometimes contain implicit, inaccurate assumptions about the state of the digital equipment that is to be tested (Klauer et al., 1993). For example, the designer may assume that the digital equipment will be tested when the plant is shut down. If the maintenance technician is not aware of these assumptions and violates them (e.g., conducting the test while the plant is operating), safety may be compromised by affecting the operation of plant systems or giving misleading results.

While improper automation of tests can introduce maintenance errors that do not typically occur during manual testing, proper use of automation can reduce certain errors and enhance maintenance. Maddox (1996) offers the following suggestions on automation in maintenance equipment used for troubleshooting:

- The automated equipment should inform maintenance personnel of what it is doing and why it is performing particular actions (e.g., indicate the condition that initiated the operation).
- The terminology used in the maintainer-test equipment interface should be compatible with the terminology used for non-automated troubleshooting tasks.
- The maintainer-test equipment interface should be consistent across all automated troubleshooting equipment.
- Understanding the information, instructions, and labels should not require the user to have software expertise.
- The maintainer-test equipment interface should display information in an easily interpreted format. Maintenance personnel should not have to examine individual bits and bytes of data to acquire troubleshooting information.
- The automated equipment should allow maintenance personnel to override automated testing or troubleshooting functions.

5.4.3.3 Built-In Test Equipment (BITE)

BITE has been used for many years to support diagnosis of electronic equipment. In the commercial aviation industry, its capabilities have evolved with those of digital aircraft systems. Examining the experiences of the aviation industry can be valuable because BITE can change maintenance tasks, especially troubleshooting activities, by making some easier and others more difficult. Hessburg (1992) provides a brief history of the evolution of BITE in commercial aircraft and describes problems in using this equipment from the perspective of an aircraft-maintenance mechanic. Three phases of BITE are described: analog, early digital, and centralized digital.

Analog BITE Systems – BITE systems used in the 1960s and early 1970s used analog technologies to assess faults in aircraft systems. Monitoring features were contained in the individual boxes of the aircraft system. Each box was directly tested by the maintainer, often by pressing a button on its front to start the test. Because each box may have been designed by a different supplier, results were not presented in a standard way. For example, fault information might be presented as red and green colored lights, patterned light codes, alpha codes, or alphanumeric codes. Also, the information provided by these systems was specific to the individual boxes; information on the overall system was not provided. Therefore, these BITE systems were confusing and hard to use. Maintenance personnel came to distrust them because the fault indications did not correlate with the actual faults.

Early Digital BITE – These systems used digital systems to test for failures. As engineers and maintenance personnel demanded more diagnostic information, more boxes and variables were monitored. However, these early digital BIT systems had problems; they locked up, and individual manufacturers used different indications for faults. In addition, fault-consolidation logic was problematic; fault messages were not always consolidated into accurate reports identifying the root cause of the malfunction. The processing logic of the fault messages did not account for the subtle relationships between systems. Individual components were falsely identified as being defective due to cascading faults, where the true failure was located in an upstream component that fed data to the tested component. In addition, nuisance messages frequently occurred. One drawback was that aircraft electronics were sensitive to conditions such as power interruptions and voltage transients. The monitoring circuits of the BITE had time delays that were insufficient for preventing them from generating fault messages during these temporary conditions. Therefore, test results were not reliable in identifying the type and location of the fault.

Centralized Digital BITE – This current phase is marked by the use of a central maintenance computer that communicates with individual sensors and testing features. This offers a number of benefits. First, the maintainer is relieved of the burden of checking individual boxes for failures because there is a central indication. Second, maintenance messages are easier to read and interpret because they are presented in English on a CRT, rather than in arcane BITE codes on distributed display devices. Third, the central computer provides better fault consolidation because the processing logic can take into account subtle relationships between different fault indications. However, centralized BIT systems have had some negative effects on maintenance personnel because they monitor many more variables and generate more messages, including some that may not be of interest to technicians. The resulting high volume of messages has overwhelmed maintenance personnel. Searching the messages to find those that are useful for diagnosing the condition of the equipment can be difficult. Furthermore, these computerized BITE systems have multiple operating modes, adding to the complexity of their operation. Although more maintenance messages are shown in English, the use of abbreviations has confused personnel. These problems add to the cognitive complexity of the maintenance task.

A current practice in the nuclear industry is to replace analog subsystems with digital equipment, rather than replacing the entire system, so that a plant system may contain individual digital components with separate BIT capabilities. For example, upgrading a feedwater control system may involve replacing some components with new digital components. While the different components are electrically compatible, they may have different user interfaces for maintainers and different test capabilities. This arrangement may be similar to the earlier BITE systems of commercial aircraft. For example, individual digital components may be tested differently and may not indicate the status of the system overall.

5 DEVELOPMENT OF TECHNICAL BASIS

Based on lessons learned from earlier BIT systems, the Boeing commercial aircraft organization established principles to guide the development of the On-board Maintenance System for the Boeing 777 aircraft (Hessburg, 1992). They fall into two categories: those pertaining to the design process, and those pertaining to the maintainer-system interface.

For the design process, an important principle is to clearly define the primary user and focus on that person's needs during the process. This principle has important implications for computer-based maintenance systems because they may be used by many personnel in addition to those who test and repair the systems, including maintenance schedulers, inventory-control personnel, trainers, and managers. The flexibility of computer technologies can encompass many different types of information and capabilities. This flexibility may result in a system that is too complicated to be operated quickly and easily by maintenance staff in the field. In developing the On-board Maintenance System, the users and their needs were carefully defined in a user requirements document. When design conflicts arose, this document was used to resolve them in favor of the primary user – the maintenance mechanic – rather than trying to provide every type of information and capability for every user. Also, the primary users were involved in the design process.

With regard to the maintainer-system interface, it was recognized that interface management (O'Hara, Stubler, and Nasta, 1997) places significant demands on users and can distract them from the primary task of maintaining the equipment. The Boeing 777 aircraft has multiple, built-in maintenance systems. A design strategy was to provide a single user interface for interacting with these systems to reduce the amount of learning and mental effort required. A single interface can avoid the need for the user to learn how each different system is organized and operated. Users should not have to keep track of which system or application is currently open. A related principle was to reduce the need for special skills that differed from those that maintenance personnel already possess; thus, typing skills were not a requirement.

Hessburg (1992) made suggestions for designing diagnosis messages for the On-board Maintenance System that are applicable to most automated test equipment, including built-in and external systems. We describe them below in terms more applicable to NPP maintenance.

- *Provide messages only if they add value to the maintenance process* – The flexibility of computer-based technologies readily allows variables to be added to the design with relative ease, compared to analog systems. Also, the needs of secondary users of the maintenance system may differ from those of the maintenance technician. Consequently, variables and capabilities may be incorporated that do not support the performance of primary users. The strategy of limiting messages to those that add value to the maintenance process is consistent with general HSI design review principle, Simplicity of Design, in Appendix A of NUREG-0700, Rev. 1, "The HSI should represent the simplest design consistent with functional and task requirements" (O'Hara, Brown, Stubler, Wachtel, and Persensky, 1996, p. A-2).

- *Do not provide messages for variables that can be monitored directly* – BIT systems can be designed to monitor many different variables, including some that are easily checked by direct observation. If a BIT system contains many variables, then a high degree of interface management may be demanded to find and use particular data. Also, when a BIT system indicates a failure, the maintainer must determine whether it reflects the system being monitored or the BIT system. Limiting the number of variables in the BIT system to those that aid maintenance, can ensure that maintenance personnel can use automated test equipment effectively. In addition, direct observation of systems can reduce uncertainty since failure of the BIT system is not considered. However, having variables in a BIT system confers some advantages in reducing the need for personnel to remember particular variables that must be monitored and can reduce the amount of effort required to check them. Also, a well-designed user interface can minimize the workload associated with managing it. Thus, the decision to include variables that could otherwise be monitored directly should take into account both the likelihood and consequences of errors associated with direct observation, and the associated costs. This approach is consistent

with the high-level HSI design review principle, Task Compatibility, NUREG-0700, Rev. 1, "The system should meet the requirements of users to perform their tasks, including maintenance and repair. There should be no unnecessary information" (O'Hara, Brown, Stubler, Wachtel, and Persensky, 1996, p. A-2; also see Appendix A of this report).

- *Define the root cause of the failure* – This suggestion addresses the situation in which automated test equipment indicates a problem but does not give sufficient information to identify the failure at the level of a specific replaceable unit. Hessburg suggests that if the root cause of the failure cannot be identified unequivocally, the test equipment should make this fact known and merely state what is known. This practical suggestion is consistent with the high-level HSI design review principle, Task Compatibility, of NUREG-0700, Rev. 1, "The system should meet the requirements of users to perform their tasks, including maintenance and repair. Data should be presented in forms and formats appropriate to the task" (O'Hara, Brown, Stubler, Wachtel, and Persensky, 1996, p. A-2).

- *Tell the maintainer what to do to fix the problem* – This suggestion addresses the significance of a failure to the maintainer's role. Thus, in addition to identifying which component has failed, the automated test system should inform personnel of the types of actions required. For example, even though component A has failed, the corrective action may require replacing components B, C, and D as well. Actions required to return the systems to service should be distinguished from those required to fix the failed component. For example, the system may be returned to service by replacing a circuit board, but repairing the circuit board may involve a separate set of tests. For NPPs, returning a system to service is important to safety because its unavailability may decrease the plant's depth of defense against additional failures. Fixing a failed component that has been removed from the system may be a lesser consideration. Thus, this suggestion is generally consistent with the high-level HSI design review principle, Task Compatibility, NUREG-0700, Rev. 1. However, the level of detail of the instructions should be consistent with the maintainer's task. For example, giving complete instructions for repair may be inappropriate if the maintainer's job merely requires the removal and replacement of components. Detailed instructions for fixing the failure in the component should be available to personnel responsible for doing so.

- *Use simple English* – Messages generated by automated test equipment should require a minimum of interpretation; they should not use abbreviations, contractions, and numeric codes. Some automated test equipment shows failure messages as numerical codes. For example, the computerized fault-reporting system of the F-15 aircraft generates a 23-digit fault code number, identifying the affected component and the technical data needed to repair it (Nondorf, 1992). Often, maintenance personnel must read these codes from the test equipment and then look up their explanation in separate tables. This process is susceptible to errors made by maintenance personnel in reading, recording, and looking up the codes. Using simple English is consistent with the high-level HSI design review principle, Task Compatibility, of NUREG-0700, Rev. 1.

5.4.4 Conclusions from Literature Review

From reviewing the literature we concluded that testing and troubleshooting digital systems can be very complex. Unlike many systems in NPPs, it is difficult to identify faulty components in digital systems by inspecting their physical characteristics; instead, diagnosis is largely symptom based. Tests are performed to see how the digital system behaves. When it does not respond properly, hypotheses must be generated about the types of failures that could result in the observed symptoms. Test equipment supports such testing.

ATE is often used when many tests are required. ATE was developed to improve the speed and accuracy of these tests. However, ATE can be complex and using it may impose special demands on maintenance personnel. For example, when both the test equipment and plant systems have multiple modes, the maintainer must ensure that the proper system mode is being tested using the appropriate test equipment mode, a challenging task if either can

change modes automatically. Using automation in test equipment puts the maintainer in a supervisory role. Rather than doing the tests, the maintainer must watch over the test equipment while it performs its tests and must ensure that they are carried out properly. Difficulties may arise if the test equipment does not give sufficient feedback to allow the maintainer to oversee its operation. There may be additional problems if the design of the test programs is not consistent with the characteristics of the test environment, or if they are too inflexible to allow the maintainer to address special exceptions.

Test equipment is built into many digital systems. Computer-based BIT systems may have very sophisticated capabilities that encompass more than one type of user. Experience in the aviation industry has shown that when BITE designers try to address all of the needs of many users, the system may be too complex or awkward to adequately support the primary user – the maintenance technician. Maintenance personnel may face high demands in interpreting fault messages. When BIT systems monitor many variables, maintenance personnel may have to search through many messages to find the right ones to diagnose a failure. In addition, the format of fault messages may affect their ability to interpret them. For example, fault messages shown as numerical codes, or text messages with abbreviations and contractions are prone to misinterpretation.

These difficulties illustrate the importance of having a systematic process for selecting or developing ATE. The type of test equipment to be used should be decided upon early in equipment design. Selection should consider many factors, including the mission and operational characteristics of plant equipment, the anticipated reliability of the plant equipment, the maintenance concept, the available personnel, the operational environment, the logistics-support requirements, and the time and cost of development (Wagner et al., 1996).

5.5 Human Performance Considerations Requiring Additional Research

In reviewing human performance considerations associated with maintaining digital systems, we identified two areas requiring further research. The first area is policies, procedures, and practices for ensuring maintainability. Industry experience indicated that procedure-related problems were a leading cause of events involving the maintenance of digital systems in NPPs. Both the basic literature and interviews with subject matter experts indicated that a systematic approach is needed to ensure that human factors considerations in maintenance are adequately addressed. Such a systematic approach should cover both the process by which maintainability features are designed into digital equipment, and the process by which the equipment is maintained. It should include the development of maintenance interfaces for digital equipment, test equipment and tools, maintenance training, and maintenance procedures.

The second area is emerging digital technologies. While guidance was obtained from the most recent HFE source documents, it is recognized that digital technology evolves rapidly. The guidance in this document is based on general principles applicable to a broad range of technologies. However, in the future there may be human factors considerations related to emerging technologies that are not explicitly addressed in these guidelines.

Two strategies are proposed to address these review needs:

- Establish process-oriented guidance for reviewing maintenance policies, procedures, and practices, including developing (a) maintainability features during design, and (b) maintenance programs for ensuring that digital systems operate properly after they are installed.

- Develop supplemental human factors guidance to address specific design topics in digital technology.

These strategies are described below.

Process-Oriented Guidance – This strategy would result in the development of guidance for reviewing practices, policies, and procedures related to maintaining digital systems. The guidance would have a format similar to that of NUREG-0711, the Human Factors Engineering Program Review Model (O'Hara et al., 1994). Good HFE design principles dictate that maintainability considerations be addressed systematically during design. NUREG-0711 describes a top-down HSI design review process with 10 review elements. Guidance should be established for each of them to specifically address the maintainability of digital systems. Some specific topics include the following:

- *HFE program development* – It is difficult to incorporate useful maintainability features at the end of the equipment design process. Careful planning must ensure that maintainability is addressed systematically throughout the design process. This guidance will be directed at the goals and scope of programs that cover HFE and maintainability in the development of digital systems.

- *HSI design* – Design requirements for maintainability features and test equipment should be developed from systematic analyses of the needs of maintainers. This guidance will address HFE considerations in the development of maintainability features and test equipment for digital systems.

- *Training maintenance personnel* – While many maintenance skills are transferable to different types of equipment, troubleshooting skills tend to be more specific to particular equipment and, consequently, less transferable. In addition, certain types of traditional training are rather ineffective for the acquisition of certain maintenance skills. For example, while classroom lectures are an ineffectual way of acquiring troubleshooting skills, training simulators can be productive (Maddox, 1996). However, there are many dimensions of simulator fidelity that influence their efficiency. Guidance is needed for developing maintenance training programs, including such topics as training methods, simulator fidelity, and assessing the program's effectiveness.

- *Design of maintenance procedures and technical information for digital systems* – Plant events, such as safety system actuations, have resulted from maintenance errors. Many of these events stemmed from unanticipated interactions between the state of the plant or plant system, the type of maintenance task performed, and the types of information, aids, and tools used. Maintenance procedures are one means of controlling the combinations of these factors to reduce the likelihood and consequences of errors. In addition, correct, complete technical information is needed to support maintenance. Guidance is needed on establishing maintenance procedures, including the management of technical information, to reduce the likelihood and consequences of mistakes and slips during maintenance work.

- *Automated test equipment and maintenance aids* – Automated test equipment has become an important tool for testing digital systems. These are usually programmable devices that execute a set of tests in rapid succession, and may have advanced capabilities for diagnosing failures. These capabilities are likely to increase in complexity and sophistication as more digital system upgrades are introduced in NPPs. Computer-based maintenance aids may be used for such functions as tracking adherence to technical specifications when removing plant equipment from service, tracking regulatory requirements, storing and analyzing system performance and maintenance data, scheduling maintenance, and tracking replacement parts. Errors in using maintenance aids may range from employing incorrect technical data, to scheduling problems, such as failing to carry out a surveillance test. Guidance is needed for reviewing the processes by which automated test equipment and maintenance aids are implemented and maintained in NPPs.

- *Verification and validation of maintenance* – Plant safety may be affected by incidents that occur during maintenance, especially that undertaken while the plant is at power. Maintenance practices that pose threats to plant safety should be evaluated through verification and validation tests to ensure that they can be done safely. This guidance would provide criteria for determining when maintenance activities should be verified and validated, and criteria for assessing the acceptability of these evaluations.

Supplemental Guidance for Digital System Features and Capabilities of Digital Systems – Digital systems have features and capabilities that pose unique challenges for maintenance activities and are not explicitly addressed by existing human factors guidelines, including this report. This strategy would result in the development of additional review guidance for these unique features and capabilities. The importance of these topics is likely to grow as the nuclear industry continues to adopt newer digital technologies to replace existing equipment and upgrade plant performance. The resulting guidance would have a format similar to that used in this report and in NUREG-0700, Rev. 1. The following are specific topics included in this category of guidance:

- On-line maintenance features – Considerations include the design of HSI features that affect personnel's awareness of the status of equipment or reduce the likelihood of input errors. Alarms and displays may include features showing the availability and operating modes (e.g., test, manual control, automatic control) of plant systems. Controls may include features that reduce the likelihood of incorrect control actions, such as entering the wrong value, operating the wrong control, or causing a bump when switching control between processors.

- Advanced features of test and diagnosis equipment – This includes features for reducing sources of detection and interpretation errors, such as long, unreadable failure codes and look-up tables that can be misread.

- Circuit cards – Industry experience indicates that because digital equipment, especially printed circuit cards, often contains similar looking components located in close proximity, the likelihood of maintenance errors involving the wrong component may be increased. These errors probably will rise as NPPs install more digital systems. As maintenance personnel are required to service more digital components, more opportunities may be created for servicing the wrong component. In addition, the complexity of digital systems may make the detection of errors more difficult. Before more definitive review guidance is established, a better understanding is needed of the types of errors that occur when the wrong component on a circuit card is serviced, and the factors contributing to these errors. Further review and research is required.

- Data-bus technologies – Within digital systems, there is a trend toward transmitting signals via communication buses, rather than individual wires; connections are made via computer addresses rather than physical wire connections. This may introduce new opportunity for personnel error. For example, by inadvertently assigning the wrong addresses, signals may be sent to the wrong processors. Accordingly, higher cognitive burdens may be imposed on maintenance personnel for understanding which signals are being transmitted and the failures that may result from improper connections. Guidance is needed to review features intended to reduce these types of errors.

6 DEVELOPMENT OF GUIDANCE

This section describes the development of the review guidance. A set of guidelines was established to cover human performance considerations identified in Section 5, using the source materials discussed in Section 3. In addition, the high-level design review principles from NUREG-0700, Rev. 1, were used to support guidance development. These principles were derived previously from reviewing research and industry experience on integrating personnel and complex systems. They reflect the important design goals of (1) maximizing personnel's primary task performance (i.e., process monitoring, decision making, and control), (2) minimizing secondary task demands unrelated to the primary task (e.g., the distracting effects of tasks such as configuring a workstation), and (3) minimizing human errors and making systems more tolerant of such errors. Two important considerations in developing the guidance were its selection and format. Each are described below.

6.1 Selection of Guidance

To be included in this document, the guidance had to satisfy two criteria. First, it had to be relevant to *human performance* aspects of maintenance. Second, it had to be relevant to the maintainability of digital systems.

Relevance to Human Performance

Human performance aspects included the following:

- Characteristics of digital system maintenance that may place high or unique demands on personnel, and thus affect the ability of personnel to restore equipment to service.

- Characteristics of digital systems that may be especially susceptible to inadequate or inappropriate personnel performance (e.g., equipment characteristics that are not tolerant of human error).

While the primary focus of this guidance development was to ensure public safety, guidance to prevent certain types of injuries to maintainers also was established. This approach is consistent with the general HSI design review principle, Personnel Safety, of Appendix A of NUREG-0700, Rev. 1, which states that HSI design should minimize the potential for injury and exposure to harmful materials. In addition, it was recognized that some types of injuries to maintenance personnel could result in damage to plant equipment, and therefore, affect plant safety. For example, injuries due to electrical shocks or contact with a hot surfaces may cause sudden motions by personnel that cause plant components to be damaged. Thus, guidance addressing these types of injuries was included.

We did not develop guidance for characteristics of digital systems that did not relate directly to personnel performance. For example, some source documents had guidance representing good electrical design practices, such as the recommended use of various types of fuses in different types of electrical circuits. Such information was not included in this document unless it pertained to special demands on maintenance personnel or to design characteristics especially sensitive to the actions of maintainers.

Relevance to Digital Systems

Guidance was developed for topics relevant to the maintainability of digital systems. If a maintenance topic was relevant to *both* digital and analog systems, it was included in this guidance development effort. However, if a maintenance topic was relevant to analog systems but not to digital systems, then it was excluded. In addition, the guidance development effort focused on activities requiring personnel interaction with digital systems, such as testing, troubleshooting, disassembling and reassembling, servicing and adjustment, and replacement and repairing. General activities, such as site preparation and cleanup, information handling, and transporting equipment, were not addressed.

Two topics closely related to maintaining digital systems were not covered. The first topic was software development. Software is an important element of digital systems and human performance plays an important role in the creation, debugging, and maintenance of software. The second topic was configuration management for digital systems (e.g., adjusting the performance of plant systems via changes to control system software). However, each of these topics is being addressed in other NRC guidance development work.

6.2 Format of Guidelines

These guidelines were developed in the standard format adopted in NUREG-0700, Rev. 1. An example is presented below:

> **9.1.1-8 Overall Accessibility**
> Equipment that is to be maintained should be visually and physically accessible to the maintainer.
> ADDITIONAL INFORMATION: Modules, components, parts, adjustment points, test points, cables, and connectors for all required maintenance tasks should be visually and physically accessible. Labels should be easily seen.
> *Discussion:* This guideline was derived from Wagner et al. (1996), 6.10.1.1 and 6.15.1.3.1.

Each guideline is composed of the following components:

- *Guideline Number* – Within each section, individual guidelines are numbered consecutively. Each guideline has a number which reflects its section and subsection location, followed by a dash and then its unique number.

- *Guideline Title* – Each guideline has a brief, unique, descriptive title.

- *Review Criterion* – Each guideline contains a statement of an HSI characteristic so that the reviewer may judge the HSI's acceptability. The criterion is not a requirement, and discrepant characteristics may be judged acceptable based on the procedures in the review process.

- *Additional Information* – For many guidelines, additional information is given which may include clarifications, examples, exceptions, details on measurements, figures, and tables. This information is intended to support the reviewer's interpretation or application of the guideline.

- *Discussion* – This section summarizes the technical basis on which the guideline was developed. It may identify the primary source documents, the technical literature, such as journal articles, or the general principle from which the guideline was derived. This section will be removed when the guidance is integrated into NUREG-0700, Rev.2.

In place of the Discussion section will be a Source field:

- *Source* – The source field identifies the NUREG or NUREG/CR (or other document) containing the technical basis and development methodology for the guideline. As is the standard practice, the source field will cite this document.

The guidelines, contained in Section 9, were organized into the following sections:

- General

- Instrument Cabinets and Racks

- Equipment Packaging
- Fuses and Circuit Breakers
- Labeling and Marking
- Adjustment Controls
- Test Points and Service Points
- Test Equipment

7 SUMMARY

Many sources of information were examined during this guidance development effort. Documents included existing human factors standards and guidelines, handbooks, and reviews of industrial incidents and maintenance practices. Additional information was obtained by visiting sites that used digital systems, and by interviewing subject matter experts from multiple domains either in-person or via telephone.

Based on our review, we concluded that the unique characteristics of digital systems can pose significant maintenance challenges. Computer-based processors, the key features of digital systems, add a degree of complexity that may not have existed in earlier I&C systems (Lee, 1994). Many interconnections can exist between digital components, subsystems, and systems, so that a single fault may affect many parts of a digital system. In some cases, the failure of a seemingly insignificant device, such as a ribbon on a peripheral printer, can start a cascade of failures that affect overall system performance (Ragheb, see Footnote 1). Also, the automatic capabilities of digital systems can change the system's configuration without direct input from personnel. For example, digital systems can automatically switch control capabilities between redundant processors but give little indication to maintenance personnel. Also, because software is a key component of digital systems, digital systems are highly susceptible to failures from software-related problems, such as its incorrect installation. In some cases, the effects of software-related problems are immediately apparent, such as when they actuate a safety system. In other cases, the effects may not be immediately apparent and may result in inoperable or improperly operating systems that provide few indications of their condition. Another result may be undesirable system behavior that is triggered when a particular combination of conditions occurs.

With these characteristics, digital systems may be more susceptible to mistakes and slips during maintenance than conventional analog equipment. Mistakes can result from incorrect assessments of situations due to the subtlety of some operating and failure modes of digital systems. Thus, plant personnel may fail to notice automatic transfers of control between redundant processors. Such errors during maintenance have resulted in safety system actuations. Mistakes can also result if maintenance is inadequately planned. This may occur when maintenance and operations personnel fail to fully consider the unique characteristics of digital systems. Because of the complex relationships between components, subsystems, and systems, maintenance work can produce unexpected interactions within them. Predicting these interactions can be very demanding, so a formal analysis should be undertaken before conducting maintenance. Additional, informal analyses of conditions and effects may be required when troubleshooting, removing, replacing, and restarting (rebooting) equipment. Contributing factors may include inadequate or incomplete maintenance procedures and technical information from vendors.

The unique characteristics of digital systems can make them highly susceptible to failures from improperly executed but correctly planned actions (slips). Some slips include failure to follow steps properly (e.g., when rebooting a processor during on-line maintenance), mode errors (e.g., failure to recognize the current system mode), keying errors, and connection errors (e.g., connecting test equipment to the wrong port or wrong system). Some of these slips may reflect the poor transfer of maintenance skills learned on older equipment. For example, rebooting digital equipment may be quite different from restarting comparable analog equipment.

Troubleshooting is one area of maintenance that has been extensively studied in human factors research. Isolating a fault to a particular component within a digital system can impose high cognitive demands, requiring an extensive knowledge of the digital system and a great degree of troubleshooting skill. Demands on long-term memory, including recalling heuristics, testing practices, and unique characteristics of the equipment, may be quite high and may result in errors. In addition, the need to remember symptoms and organize test hypotheses can impose high demands on short-term and working memory. However, the human performance concerns associated with troubleshooting digital equipment appear to have more of an economic effect than a safety one for the nuclear industry. Because digital equipment is modular, malfunctions can be readily corrected by replacing circuit boards and other parts until the failure is found. Thus, the affected system can be rapidly restored to proper operation, and the task of troubleshooting the removed piece of equipment can be performed later.

7 SUMMARY

Troubleshooting can place high demands on the maintenance organizations of NPPs. Many resources, including personnel, test equipment, materials, and time, may be devoted to trying to identify faults in the components removed from plant systems. For many of them, the original test results indicating that the component is faulty cannot be duplicated. As a result, the fault may never be found. This represents a drain on human resources, which may indirectly affect plant safety. If resources are diverted to troubleshooting, then fewer resources may be available for properly maintaining other equipment in the plant. Thus, off-line troubleshooting may *indirectly* threaten plant safety. However, other concerns, such as preventing mistakes and slips, may challenge plant safety more directly.

The human factors considerations associated with digital systems can be addressed in many ways. Design-oriented solutions may be applied to the maintenance-system interfaces of digital equipment and test devices to reduce maintenance errors. Administrative solutions may be applied in selecting and training of maintenance personnel and developing maintenance procedures.

The guidance in Part 2 was derived from the latest available documents with the highest internal and external validity. Extensive use was made of existing standards and guidelines that have undergone peer review. The guidance reflects the current knowledge of human capabilities and limitations that can affect the performance of maintenance tasks. This guidance is primarily design-oriented, consistent with other HSI guidance in NUREG-0700, Rev. 1. Its primary focus is on the interfaces with which personnel interact when performing maintenance. It is organized in eight sections addressing the following topics: general considerations, instrument cabinets and racks, equipment packaging, fuses and circuit breakers, labeling and marking, adjustment controls, test points and service points, and test equipment.

Some topics support maintenance personnel in understanding the arrangement and status of components in digital systems; this guidance may reduce the likelihood of mistakes. For example, the topic, packaging of internal components, provides guidance for organizing digital equipment into individual modules to support maintenance personnel in searching for and isolating malfunctions. The topic, adjustment controls, provides guidance to ensure that maintenance personnel have adequate feedback when adjusting plant equipment. The topics, failure detection and isolation and test equipment, consider the presentation of test information to support personnel in detecting faults. Some topics represent good design practices that may reduce the likelihood of inadvertent actions (slips). For example, the packaging topic contains guidelines for preventing modules from being installed incorrectly and preventing functionally different modules from being interchanged. The labeling and marking topic contains guidelines that ensure that test points, service points, and components are properly designated to reduce their likelihood of being incorrectly identified by the maintainer. In addition, many topics contain good design practices to improve the overall efficiency of maintenance. This can improve system availability by reducing the time required for surveillance tests, preventive maintenance, and corrective maintenance. Thus, these guidelines encompass many of the maintenance problems identified in Section 5.

Two areas that require further research for developing review guidance were identified in Section 5.5: (1) policies, procedures, and practices for ensuring maintainability, and (2) specified design topics in digital technology. For the first, we propose further research to develop process-oriented guidance, in a format compatible with NUREG-0711. Guidance should be developed for each of the 10 elements of NUREG-0711 to specifically address considerations related to the maintainability of digital systems. The following are some of the specific topics included: HFE program development, HSI design, training, procedures, the development of automated test equipment and maintenance aids, and verification and validation of maintenance.

For the second area, it is proposed that further research be conducted to develop supplemental human factors guidance on specific digital technologies; its format would be consistent with the guidance in Section 9 of this report and NUREG-0700, Rev. 1. While the guidance presented in this document is based on principles applicable to a broad range of technologies, digital technology continues to evolve at a rapid rate. Hence, human factors

considerations related to the features of digital systems that are not explicitly addressed in Section 9 may be encountered in the future. The following topics were identified as being particularly important to maintaining digital systems: features that support on-line maintenance, advanced features of test and diagnosis equipment, and features of circuit cards and data buses that are related to maintenance errors.

8 REFERENCES

Badalamente, R., Fecht, B., Blahnik, D., Eklund, J., and Hartley, C. (1986). *Recommendations to the NRC on human engineering guidelines for nuclear power plant maintainability* (NUREG/CR-3517). Washington, DC: U.S. Nuclear Regulatory Commission.

Bennetts, R. (1984). *The design of testable logic circuits*. Reading, MA: Addison-Wesley.

Bongarra, J., Van Cott, H., Pain, R., Peterson, L., and Wallace, R. (1985). *Human factors design guidelines for maintainability of Department of Energy Nuclear Facilities* (Tech. Report UCRL-15673). Livermore, CA: Lawrence Livermore National Laboratory.

EPRI (1992). *Advanced light water reactor utility requirements document. Volume II: ALWR evolutionary plant.* (Chapter 10, Man-Machine Interface Systems). Palo Alto, CA: Electric Power Research Institute.

EPRI (1993). *Advanced light water reactor utility requirements document. Volume III: ALWR passive plant,* (Chapter 10, Man-Machine Interface Systems). Palo Alto, CA: Electric Power Research Institute.

Galyean, W. (1994). *Digital control systems in nuclear power plants: Failure information, modeling concepts, and applications* (Tech. Report EGG-2740). Idaho Falls, ID: Idaho National Engineering Laboratory.

Hessburg, J. (1992). Human factors considerations of the 777 on board maintenance system design. In J. Parker, Jr. and A. White (Eds.), *Proceedings of the Sixth Meeting on Human Factors Issues in Aircraft Maintenance and Inspection*. Washington, DC: Office of Aviation Medicine, Federal Aviation Administration.

Johansson, E. (1996). Retrofitting I&C systems in Swedish nuclear power plants: Fundamental issues enlightened. In *Proceedings of the 1996 American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies.* La Grange, IL: American Nuclear Society.

Johnson, W. and Rouse, W. (1982). Training maintenance troubleshooting: Two experiments with computer simulation. *Human Factors, 24*, 271-276.

Klauer, K., Gravelle, M., Schopper, A., and Howell, L. (1993). *Test and maintenance of digital systems* (Tech. Report CSERIAC-RA-93-9015). Wright-Patterson AFB, OH: Crew System Ergonomics Information Analysis Center.

Lee, E. (1994). *Computer-based digital systems failures* (Technical Review Report AEOD/T94-03). Washington, DC: U.S. Nuclear Regulatory Commission.

Licensee Event Report 50-219/94-021 (1994). *Automatic reactor scram due to high reactor recirculation flow caused by personnel error.*

Licensee Event Report 50-423/93-008 (1993). *Main steam valve building temperature monitor inoperable.*

Licensee Event Report 50-413/93-008 (1993). *Reactor trip and auxiliary feedwater system automatic start.*

Licensee Event Report 50-311/90-008 (1990). *ESF actuation - Containment ventilation isolation due to inadvertent personnel error.*

Lewis, C. and Norman, D. (1986). Designing for error. In D. Norman and S. Draper (Eds.), *User-centered system design*. Hillsdale, NJ: Erlbaum.

8 REFERENCES

Maddox, M. (1996). *Human factors guide for aviation maintenance*, Version 2.0. (GPO Document 050-007-01098-2). Washington, DC: U.S. Government Printing Office.

Maddox, M. (1996). Testing and troubleshooting. In M. Maddox (Ed.), *Human factors guide for aviation maintenance, Version 2.0.* (GPO Document 050-007-01098-2). Washington, DC: U.S. Government Printing Office.

Majoros, A. and Boyle, E. (1997). Maintainability. In G. Salvendy (Ed.), *Handbook of human factors*. New York: Wiley.

Mitchell, C. and Williams, K. (1993). Failure experience of programmable logic controllers used in emergency shutdown systems. *Reliability Engineering and System Safety, 39*, 329-331.

NASA (1995). *Man-system integration standards* (NASA-STD-3000B). Washington, DC: National Aeronautics and Space Administration.

NASA (1987). *Man-system integration standards* (NASA-STD-3000). Washington, DC: National Aeronautics and Space Administration.

National Research Council (1997). *Digital instrumentation and control systems in nuclear power plants: Safety and reliability issues.* Washington, DC: National Academy Press.

Nondorf, T. (1992). Maintenance advances in the F-15 aircraft program. In J. Parker, Jr. and A. White (Eds.), *Proceedings of the Sixth Meeting on Human Factors Issues in Aircraft Maintenance and Inspection*. Washington, DC: Office of Aviation Medicine, Federal Aviation Administration.

Norman, D. (1983). Design rules based on analyses of human error. *Communications of the ACM, 26*, 254-258.

Norman, D. (1981). Categorization of action slips. *Psychological Review, 88*, 1-15.

NRC (1996). *Information notice 96-56: Problems associated with testing, tuning, or resetting of digital controls while at power*. Washington, DC: U.S. Nuclear Regulatory Commission.

NRC (1994). *NRC review of Electric Power Research Institute's advanced light water reactor utility requirements document*, Chapter 10 Man-Machine Interface Systems (NUREG-1242, Vol. 3, Part 2). Washington, DC: U.S. Nuclear Regulatory Commission.

NRC (1993). *Information notice 93-49: Improper integration of software into operating practices.* Washington, DC: U.S. Nuclear Regulatory Commission.

NRC (1985a). *Status of maintenance in the U.S. nuclear power industry 1985, Volume 1: Findings and conclusions* (NUREG-1212, Vol. 1). Washington, DC: U.S. Nuclear Regulatory Commission.

NRC (1985b). *Status of maintenance in the U.S. nuclear power industry 1985, Volume 2: Description of programs and practices* (NUREG-1212, Vol. 2). Washington, DC: U.S. Nuclear Regulatory Commission.

NRC (1973). *Bypassed and inoperable status indication for nuclear power plant safety systems* (Regulatory Guide 1.47). Washington, DC: U.S. Nuclear Regulatory Commission.

O'Hara, J., Brown, W., Stubler, W., Wachtel, J., and Persensky, J. (1996). *Human-system interface design review guideline* (NUREG-0700, Rev. 1). Washington, DC: U.S. Nuclear Regulatory Commission.

O'Hara, J., Higgins, J., Stubler, W., Goodman, C., Eckenrode, R., Bongarra, J., and Galletti, G. (1994). *Human factors engineering program review model* (NUREG-0711). Washington, DC: U.S. Nuclear Regulatory Commission.

O'Hara, J., Stubler, W., and Nasta, K. (1997). *Human-system interface management: Effects on operator performance and issue identification* (BNL Technical Report W-6546-1-1-7/97). Upton, NY: Brookhaven National Laboratory.

O'Hara, J., Stubler, W., and Higgins, J. (1996). *Hybrid human-system interfaces: Human factors considerations* (BNL Technical Report J6012-T1-4/96). Upton, NY: Brookhaven National Laboratory.

O'Hara, J., Brown, W., and Nasta, K. (1996). *Development of the human-system interface design review guideline: NUREG-0700, Revision 1* (BNL Technical Report L-1317-2-12/96). Upton, NY: Brookhaven National Laboratory.

Pack, R., Seminara, J., Shewbridge, E., and Gonzalez, W. (1985). *Human engineering design guidelines for maintainability* (Tech. Report EPRI NP-4350). Palo Alto, CA: Electric Power Research Institute.

Paula, H. (1993). Failure rates for programmable logic controllers. *Reliability Engineering and System Safety, 39,* 325-328.

Paula, H., Roberts, M., and Battle, R. (1993). Operational failure experience of fault-tolerant digital control systems. *Reliability Engineering and System Safety, 39,* 272-289.

Reason, J. (1990). *Human error*. New York: Press Syndicate of the University of Cambridge.

Reason, J. and Maddox, M. (1996). Human error. In M. Maddox (Ed.), *Human factors guide for aviation maintenance, Version 2.0.* (GPO Document 050-007-01098-2). Washington, DC: U.S. Government Printing Office.

Roth, E., Elias, G., Mauldin, M., and Ramage, W. (1985). Toward joint person-machine cognitive systems: A prototype expert system for electronics troubleshooting. In *Proceedings of the Human Factors Society 29th Annual Meeting*. Santa Monica, CA: Human Factors Society.

Samanta, P., Kim, I., Mankamo, T., and Vesely, W. (1994). *Handbook of methods for risk-based analyses of technical specifications* (NUREG/CR-6141). Washington, DC: U.S. Nuclear Regulatory Commission.

Sarter, N. and Woods, D. (1995). How in the world did we ever get into that mode? Mode error and awareness in supervisory control. *Human Factors, 37,* 5-19.

Stubler, W., O'Hara, J., and Kramer, J. (2000). *Soft controls: technical basis and review guidance* (NUREG/CR-6635). Washington, DC: U.S. Nuclear Regulatory Commission.

Stubler, W., Higgins, J., and O'Hara, J. (1996). *Evaluation of the potential safety significance of hybrid human-system interface topics* (BNL Technical Report J6012-T2-6/96). Upton, NY: Brookhaven National Laboratory.

Stubler, W. and O'Hara, J. (1996). *Proposed guidance development for hybrid human-system interface issues* (BNL Technical Report J6012-T3-10/96). Upton, NY: Brookhaven National Laboratory.

Teague, R. and Allen, J. (1997). The reduction of uncertainty and troubleshooting performance. *Human Factors, 39,* 254-267.

8 REFERENCES

Toms, M. and Patrick, J. (1987). Some components of fault-finding. *Human Factors, 29*, 587-597.

Toms, M. and Patrick, J. (1989). Components of fault-finding: Symptom interpretation. *Human Factors, 31*, 465-483.

U.S. Department of Defense (1997). *Identification markings of U.S. military property* (MIL-STD-130J). Philadelphia, PA: Navy Publishing and Printing Office.

U.S. Department of Defense (1985). *Standard general requirements for electronic equipment* (MIL-STD-454). Philadelphia, PA: Navy Publishing and Printing Office.

Wagner, D., Birt, J., Snyder, M., and Duncanson, J. (1996). *Human factors design guide (HFDG): For acquisition of commercial off-the shelf subsystem, non-developmental items, and developmental systems* (Tech. Report DOT/FAA/CT-96/1). Springfield, VA: National Technical Information Service.

Watterson, J., Royals, M., and Kanopoulos, N. (1992). *Chip-level testability requirements guidelines* (Tech. Report RL-TR-92-309 / AD-A262 583). Ft. Belvoir, VA: Defense Technical Information Center.

Wermiel, J. (1997a). *Computer-based digital systems failures: April 1997 - August 1997* (Memo to L. Spessard, dated October 16, 1997). Washington, DC: U.S. Nuclear Regulatory Commission.

Wermiel, J. (1997b). *Computer-based digital systems failures: December 1996 - March 1997* (Memo to B. Boger, dated April 28, 1997). Washington, DC: U.S. Nuclear Regulatory Commission.

Wermiel, J. (1996a). *Computer-based digital systems failures: September 1996 - November 1996* (Memo to B. Boger, dated December 31, 1996). Washington, DC: U.S. Nuclear Regulatory Commission.

Wermiel, J. (1996b). *Computer-based digital systems failures: June 1996 - August 1996* (Memo to B. Boger, dated September 30, 1996). Washington, DC: U.S. Nuclear Regulatory Commission.

Wermiel, J. (1996c). *Computer-based digital systems failures : March 1996 - June 1996* (Memo to B. Boger, dated June 24, 1996). Washington, DC: U.S. Nuclear Regulatory Commission.

Wermiel, J. (1996d). *Computer-based digital systems failures: December 1995 - February 1996* (Memo to B. Boger, dated March 14, 1996). Washington, DC: U.S. Nuclear Regulatory Commission.

Wermiel, J. (1995a). *Computer-based digital systems failures: June 1995 - August 1995* (Memo to B. Boger, dated September 18, 1995). Washington, DC: U.S. Nuclear Regulatory Commission.

Wermiel, J. (1995b). *Computer-based digital systems failures: March 1995 - May 1995* (Memo to B. Boger, dated June 13, 1995). Washington, DC: U.S. Nuclear Regulatory Commission.

Wermiel, J. (1995c). *Computer-based digital systems failures* (Memo to B. Boger, dated March 28, 1995). Washington, DC: U.S. Nuclear Regulatory Commission.

Wiener, E. and Nagel, D. (1988). *Human factors in aviation.* San Diego, CA: Academic Press.

PART 2:

Guidance for Maintainability Review

9 HFE DESIGN REVIEW GUIDELINES FOR DIGITAL SYSTEM MAINTAINABILITY

The guidelines in this section reflect the characterization of digital systems and associated maintenance aids discussed in Section 4. They also reflect the findings of our literature review on maintenance of digital systems, specifically the human performance considerations in Section 5. As described in the procedure for HSI design review presented in Part 1 of NUREG-0700, Rev. 1, the first step in a design review is to select the subset of guidelines relevant to the particular design. It is recognized that there is a wide range of digital systems, test equipment, and information aids. Sometimes, not all of the characteristics and functions addressed in these guidelines may be present. For individual reviews, the reviewer might wish to use the characterization from Section 4 to identify important characteristics that are to be evaluated using the guidelines.

As described in Section 6, guidelines were developed from the findings and source materials reviewed in Section 5. They were constructed in the standard format adopted in NUREG-0700, Rev. 1. The guidelines are organized into the following sections:

- General
- Instrument Cabinets and Racks
- Equipment Packaging
- Fuses and Circuit Breakers
- Labeling and Marking
- Adjustment Controls
- Test Points and Service Points
- Test Equipment

These new guidelines will be integrated with the design review guidance already in NUREG-0700, Rev. 1.

9.1 General

9.1.1 Minimizing Maintenance Demands

9.1.1-1 Minimizing Testing and Servicing

Requirements for periodic or repetitive testing and servicing of components should be avoided where the possibility of human errors may affect safety.

ADDITIONAL INFORMATION: One way to reduce the need for testing and servicing is to use highly reliable components.

Discussion: This guideline was derived from Wagner et al. (1996), 6.14.2.7. Section 3.3 discusses the history of human factors guidance documents that address maintenance. Wagner et al. (1996) is the latest in a series of such documents that share a common technical basis. It is cited here because it provides the most current guidance from this series.

9.1.1-2 Equipment Independence for Maintenance

Units of equipment should be as independent as is practical, such that maintenance of one unit has minimal effects on the other equipment.
ADDITIONAL INFORMATION: Functional, mechanical, electrical, and electronic independence can allow one unit to be maintained with minimal effects on other units. Units of equipment should correspond to the functional design of the equipment. The functional independence of each unit should be maximized while minimizing the interaction between them.
Discussion: This guideline was derived from Wagner et al. (1996), 6.1.2.5. Some of the additional information was derived from Wagner et al. (1996), 6.3.1.1.

9.1.1-3 Minimize Maintenance Time
Equipment should be designed to minimize the time required for maintenance if having the equipment out of service can affect safety.
ADDITIONAL INFORMATION: Minimizing the time required for maintenance can increase the equipment's availability. One factor that can increase maintenance time is high cognitive demands associated with such activities as finding components and test or service points, tracing flows between components, and detecting and interpreting symptoms. A second factor is high physical demands, such as dexterity for disassembling and reassembling equipment, accessing internal components, and using connectors, test points, and service points. Maintenance time may also be lengthened by factors that increase the likelihood of errors, such as inadequate feedback from plant or test equipment. In addition, factors that introduce delays or special logistic requirements, such as the need for special tools and test equipment may prolong maintenance.
Discussion: This guideline was derived from Wagner et al. (1996), 6.1.5.2.

9.1.1-4 Ease of Fault Detection
The design of equipment should facilitate rapid, positive fault detection and isolation of defective items.
Discussion: This guideline was derived from Wagner et al. (1996), 6.12.3.4.

9.1.1-5 Equipment Verification
When feasible, equipment should permit verification of operational status before its installation and without the need for disassembly.
ADDITIONAL INFORMATION: For example, maintenance personnel should be able to verify that a module is in operating condition through inspections or tests, such as by attaching the equipment to a test device. These inspections and tests should not require the maintainer to disassemble the module.
Discussion: This guideline was derived from Wagner et al. (1996), 6.12.3.7.

9.1.1-6 Fault Detection Without Disassembly
Equipment should permit fault detection and isolation without removing components, through the use of BIT, integrated diagnostics, or standard test equipment.
ADDITIONAL INFORMATION: Fault detection and isolation should unambiguously identify which component has failed.
Discussion: This guideline was derived from Wagner et al. (1996), 6.12.3.8.

9.1.1-7 Design for Repair by Module Replacement
To reduce the likelihood of personnel errors in normal repairs conducted in difficult field environments, the design should support simple modular replacement in the field, and their repair in the shop.
ADDITIONAL INFORMATION: Repair activities, such as rewiring and replacing individual small components, may be more prone to errors when carried out in the field. Restricting field maintenance to replacing modules may reduce the likelihood of these errors.
Discussion: This guideline was derived from NUREG-1242 (NRC, 1994), 3.7.3.

9.1.1-8 Overall Accessibility
Equipment that is to be maintained should be visually and physically accessible to the maintainer.
ADDITIONAL INFORMATION: Modules, components, parts, adjustment points, test points, cables, and connectors for all required maintenance tasks should be visually and physically accessible. Labels should be easily seen.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.1.1 and 6.15.1.3.1.

9.1.1-9 Standardized Designs for Construction
Equipment used in assembling equipment, such as connectors, should be standardized as much as possible.
ADDITIONAL INFORMATION: Standardization reduces the need for maintainers to learn different skills for different designs, and may reduce the likelihood of errors from using the wrong technique when disassembling and reassembling equipment.
Discussion: This guideline was derived from NUREG-1242 (NRC, 1994) 3.8.3.

9.1.1-10 Design Flexibility
Equipment design should provide flexibility to allow future design modifications to be made without imposing high demands on personnel for installation and maintenance.
ADDITIONAL INFORMATION: Equipment should be designed to accommodate future modifications or replacement of equipment. Design flexibility includes functional and physical modularity to accommodate replacements and upgrades, and spare physical capacity, such as in cabinets, panels, terminal strips, and wire ways, to provide room for larger or more components. Extra electrical and processing capacity may also support the maintainability of future modifications.
Discussion: This guideline was derived from NUREG-1242 (NRC, 1994), 3.9 and EPRI (1993), 3.9.

9.1.1-11 Minimize Maintenance Equipment and Tools
Units of equipment should be designed to minimize the numbers and types of auxiliary equipment and tools required to service them.
ADDITIONAL INFORMATION: Tool requirements should be coordinated across the modules to minimize the number of different tools needed. For example, designers may design modules for the same type of screwdriver rather than requiring a slightly different one for each. The development of tool requirements requires an understanding of the maintenance tasks and the equipment's characteristics. The goal of minimizing the number and types of tools should be addressed early in the equipment design process, and then throughout design and development.
Discussion: This guideline was derived from Wagner et al. (1996), 6.1.3.4 and 6.16.1.1. The additional information was derived from Wagner et al. (1996), 6.16.

9.1.1-12 Use Common Test Equipment and Tools
Whenever possible, systems and units of equipment should be designed so they can be maintained with common test equipment and tools.
ADDITIONAL INFORMATION: The need for specialty test equipment and tools should be avoided. Ideally, the tools required should be limited to those normally found in a maintainer's tool kit. Modules should be designed so that they are replaceable by hand or with common tools.
Discussion: This guideline was derived from Wagner et al. (1996), 6.1.3.5 and 6.10.4.11

9.1.1-13 Need for Special Skills
Equipment should be designed to minimize the need for special skills on the part of the maintainers.
Discussion: This guideline was derived from NASA (1995), 12.2.d.1 and 12.3.1.1r.

9.1.1-14 Need for Special Training
Equipment should be designed to minimize the need to specially train the maintainers.

Discussion: This guideline was derived from NASA (1995), 12.2.d.2.

9.1.2 Continuous Operation and On-Line Maintenance

9.1.2-1 Local Indication of Redundant Equipment Status
If equipment can automatically transfer operation between redundant units, local personnel who maintain that equipment should be informed of the transfer and the status of the redundant units.
ADDITIONAL INFORMATION: Some digital systems automatically transfer control between redundant processors when there is a failure. These redundant processors support on-line maintenance by allowing one processor to control the system while the others are being serviced. When maintenance is performed, local maintenance personnel should be alerted when an automatic transfer occurs, and should be able to readily determine the status of the redundant processors and identify the one controlling the system. Local indications are preferable to control room indications so local personnel need not rely on operators for status information.
Discussion: Section 5.2 of this report describes NPP events that occurred during on-line maintenance of digital systems. Safety system actuations have occurred because maintenance personnel were unaware that the processor they were servicing was controlling the system, or were unaware that a transfer had not been completed. These events were partly due to a failure to adequately alert local personnel to the status of the redundant processors.

9.1.2-2 Degraded Operation
Status and fault information should be provided to maintenance personnel and operators for equipment awaiting maintenance while operating in a degraded mode.
ADDITIONAL INFORMATION: Because of their importance in a system, some units of equipment may be designed to operate in a degraded mode after a partial failure while awaiting maintenance. Degraded operation and faults should be sensed and appropriate information identified, displayed, or transmitted to maintenance personnel and operators.
Discussion: This guideline was derived from Wagner et al. (1996), 6.1.2.3.

9.1.3 Supporting the Operator Role in Maintenance

9.1.3-1 Monitoring and Trending Equipment Degradation
To support personnel awareness of impending equipment failures, monitoring and trending capabilities should be provided where possible to identify the degradation of equipment.
Discussion: This guideline was derived from NUREG-1242 (NRC, 1994), 5.6.

9.1.3-2 Operator Assistance in Testing and Repair
Where practical, equipment should be designed to facilitate testing and repairs without requiring the assistance of the on-shift operator.
ADDITIONAL INFORMATION: Maintenance activities should be designed so that they do not interrupt the operator at staffed control stations.
Discussion: This guideline was derived from NUREG-1242 (NRC, 1994), 3.7.7 and is also reflected in Regulatory Guide 1.47 (NRC, 1973).

9.1.3-3 Operator Indication of Testing or Repair Activities
The operators should be provided with an indication that testing or repairs are underway.
ADDITIONAL INFORMATION: Some testing and repairs may affect equipment or system operability or make it more susceptible to unusual events, such as spurious trips.
Discussion: This guideline was derived from NUREG-1242 (NRC, 1994), 3.7.7.

9.1.3-4 Indications for Equipment that is Out of Service

Means for indicating the status of equipment that is out of service should be provided.
ADDITIONAL INFORMATION: Administrative controls for managing these indications (i.e., for tagging-in and tagging-out equipment) also should be in effect.
Discussion: This guideline was derived from NUREG-1242 (NRC, 1994), 3.7.7 and is also reflected in Regulatory Guide 1.47 (NRC, 1973).

9.1.4 Protecting Personnel from Hazards

9.1.4-1 Designing for Safety of Maintainers

Equipment should not present hazards to maintainers as they follow maintenance procedures.
ADDITIONAL INFORMATION: A positive means (for example, disconnects or lockouts) should be designed into equipment to control hazardous conditions and increase safety. A hazardous condition is the presence of energy or a substance which is likely to cause death or injury by physical force, shock, radiation, explosion, flames, poison, corrosion, oxidation, irritation or other debilitating features.
Discussion: This guideline was derived from Wagner et al. (1996), 6.1.2.6.

9.1.4-2 Covering Exposed Parts

Protrusions and corners on equipment that maintainers might come into contact with should be covered with rubber or other appropriate materials.
ADDITIONAL INFORMATION: Protrusions and corners on equipment may injure the maintainers or cause them to make sudden motions that could damage plant equipment.
Discussion: This guideline was derived from Wagner et al. (1996), 6.15.1.2.3.

9.1.4-3 Energy Dissipation Before Maintenance

Parts that retain hazardous levels of electrical potential or heat should be equipped with means to dissipate energy before to maintenance.
ADDITIONAL INFORMATION: Heat sinks and electrical grounds can be used to dissipate energy before maintenance. Removing these hazards can reduce the risk of personnel injury. It may also reduce the risk of damage to plant equipment that could result from sudden personnel movements after touching hot or electrically charged surfaces.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.3.3.5 and NASA (1995), 12.3.1.4.g.

9.1.4-4 Protecting Maintainers from Heat and Electrical Shock

Equipment or parts that retain hazardous levels of heat or electrical potential during maintenance should be located where maintainers will not touch them during their work, or they should be shielded.
ADDITIONAL INFORMATION: For example, high-current switching devices should be shielded to prevent maintainers from coming into contact with them. Internal controls, such as switches and adjustment controls, should be located away from hazardous high-voltage sources with which the maintainers may make contact while operating the controls. Shocks and burns received from equipment may injure maintenance workers or cause them to make sudden motions resulting in damage to equipment. This concern is particularly important for parts that retain energy after external energy sources have been removed or turned off.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.3.3.4, 6.10.3.3.6, and 6.10.3.3.7 and of NASA (1995), 12.3.1.4.g.

9.1.4-5 Avoidance of Hazards for Adjustment Controls, Test Points, and Service Points

Adjustment controls and test and service points should be located away from hazards.

ADDITIONAL INFORMATION: Adjustment controls and test and service points should not be located close to dangerous voltages, moving machinery, or other hazards, since contact with these hazards may injure maintenance workers or cause them to damage plant equipment by their sudden motion. They should be separated by more than a hand's width, 114 mm (4.5 in), from the nearest hazard. If a hazardous location cannot be avoided, the control, test point, or service point should be appropriately labeled, shielded, and guarded.
Discussion: This guideline was derived from Wagner et al. (1996), 6.11.20 and 6.14.5.1. The separation criteria included in the additional information was derived from Wagner et al. (1996), 6.14.5.2 and 6.14.5.1.

9.1.5 Protecting Equipment and Components from Hazards

9.1.5-1 Protecting Equipment from Hazards
Equipment should be protected from potential exterior hazards resulting from personnel actions.
ADDITIONAL INFORMATION: Protection may be provided by the design and location of equipment, or by protective barriers or enclosures. Hazards resulting from personnel actions include physical forces, contact with contaminants (such as oil), other fluids, dirt, and contact with static electricity.
Discussion: This guideline was derived from NUREG-1242 (NRC, 1994), 6.2.2 and Wagner et al. (1996), 6.10.3.3.3.

9.1.5-2 Avoiding Damage to Protruding Parts
Irregular protrusions on a unit of equipment should be easily removed to prevent damage by personnel during installation and maintenance.
ADDITIONAL INFORMATION: An electrical cable is an example of an irregular protrusion.
Discussion: This guideline was derived from Wagner et al. (1996), 6.3.1.7.

9.1.5-3 Avoiding Damage When Opening and Closing Equipment
The parts and wiring of a module should be located and arranged so that personnel do not damage them when the module or the unit of equipment of which they are part is opened and closed.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.3.3.1.

9.1.5-4 Avoiding Damage When Maintaining Internal Components
Parts that are susceptible to damage by personnel should be located or shielded so that they will not be damaged during maintenance.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.3.3.2.

9.2 Instrument Cabinets and Racks

9.2-1 Instrument Racks
Instrument racks should support maintenance and testing by providing adequate physical and visual access to their contents.
ADDITIONAL INFORMATION: Instrument racks provide a location for mounting instruments and wiring.
Discussion: This guideline was derived from NUREG-1242 (NRC, 1994), 6.2.2.

9.2-2 Cabinet Lighting
Cabinets requiring maintenance inside the enclosure should have permanent lighting.
ADDITIONAL INFORMATION: Permanently installed lighting should be an aid to personnel in diagnostics, repairs, and troubleshooting. Using hand-held lights may pose hazards for personnel or cause damage to equipment.
Discussion: This guideline was derived from NUREG-1242 (NRC, 1994), 6.2.2.

9.2-3 Minimizing Field-Run Wiring

The amount of field-run wiring should be minimized to avoid errors in identifying and connecting wires.
ADDITIONAL INFORMATION: The amount of wiring carried out in the field may be reduced by using multi-connector connections and pre-assembled wiring harnesses. Connectors may have features preventing problems such as improper indexing, electrical shorts, and inadvertent contacts.
Discussion: This guideline was derived from NUREG-1242 (NRC, 1994), 3.7.7.

9.2-4 Protective Electrical Grounds for Cabinets

A protective ground should be provided.
ADDITIONAL INFORMATION: All cabinets where the operating voltage is greater than 50 volts should have a protective ground. Protective power grounds should be routed separately from signal grounds. Inadequate electrical grounding may cause electrical shocks to plant personnel resulting in injury or sudden motion that may damage plant equipment.
Discussion: This guideline was derived from NUREG-1242 (NRC, 1994), 6.2.2.

9.3 Equipment Packaging

9.3.1 General

9.3.1-1 Organized by Maintenance Specialty

Parts and modules should be packaged, laid out, and mounted so that maintenance performed by one maintenance specialist does not require removing or handling of equipment or components maintained by another specialist.
ADDITIONAL INFORMATION: Reducing the number of maintenance specialties involved with each part or module can simplify the process, reduce the likelihood of errors and delays due to communication difficulties between specialists, and reduce the time that equipment is out of service.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.1.4.

9.3.2 Modularization

9.3.2-1 Modularization

Units of equipment should be divided into as many modules as are practical and feasible to support personnel performance during maintenance.
ADDITIONAL INFORMATION: Dividing a unit of equipment into a number of separate modules has several advantages, including making it easier to (1) locate and isolate malfunctions, (2) reach, remove, and maintain components, (3) handle the equipment for installation and repair, and (4) allocate maintenance functions and responsibilities between personnel with different skills.
Discussion: This guideline was derived from guidelines 6.1.2.7 and 6.10.2.1.1 of Wagner et al. (1996).

9.3.2-2 Physical and Functional Interchangeability

If modules are physically interchangeable, they should also be functionally interchangeable to avoid errors in installing the wrong module.
ADDITIONAL INFORMATION: Functionally interchangeable units of equipment perform the same function. Physically interchangeable units of equipment can fit into the same mounting position or fixture. If two units of equipment are interchangeable functionally, they should also be interchangeable physically. However, if they are not interchangeable functionally, they should not be interchangeable physically. Units of equipment having the same form and function should be interchangeable throughout a system and related systems.

Discussion: This guideline was derived from Wagner et al. (1996), 6.10.2.1.3. The additional information was derived from Wagner et al. (1996), 6.3.2, 6.3.2.1, and 6.1.3.2.

9.3.2-3 Distinguishing Noninterchangeable Modules

The appearance of noninterchangeable modules should be distinguishable, and the difference should be apparent when the module is in its installed position.

ADDITIONAL INFORMATION: Interchangeable units of equipment should be clearly identifiable and easily distinguishable from units that are similar, but not interchangeable. Identification methods might be physical (such as size, shape, and mounting provisions) or visual (such as color coding and labeling).

Discussion: This guideline was derived from Wagner et al. (1996), 6.10.2.1.4. Additional information was derived from Wagner et al. (1996), 6.3.2.2.

9.3.2-4 Replacement of Failed Components

Equipment should be designed so that components that fail frequently can be easily replaced.

ADDITIONAL INFORMATION: Lamps and fuses are examples of parts that fail more frequently.

Discussion: This guideline was derived from Wagner et al. (1996), 6.1.2.9.

9.3.2-5 Maintenance in Installed Location

When possible, modules should be designed so that they can be maintained in their installed position, without requiring disconnection, disassembly, or removal of other modules.

Discussion: This guideline was derived from Wagner et al. (1996), 6.10.2.1.6.

9.3.2-6 Unreliable Components

If a module has parts that are significantly less reliable than the remaining ones, the unreliable parts should be accessible without removing the module.

Discussion: This guideline was derived from Wagner et al. (1996), 6.10.2.1.5.

9.3.2-7 Removal and Testing

Modules should be designed to permit testing when they are removed from their installed position.

ADDITIONAL INFORMATION: Personnel should not be required to re-install a module into the system to determine whether it has failed, because errors may occur during installation. Other system characteristics also may mask faults in the module. These problems may be avoided by testing the module directly.

Discussion: This guideline was derived from Wagner et al. (1996), 6.10.2.1.7.

9.3.2-8 Installation and Testing

Each module should allow separate installation and functional testing before the complete system is integrated.

ADDITIONAL INFORMATION: The design should allow maintenance personnel to test and confirm that the installed module is functioning properly before the complete system is installed.

Discussion: This guideline was derived from NUREG-1242 (NRC, 1994), 3.7.7.

9.3.2-9 Installation and Calibration

Modules should require little or no calibration immediately after installation.

Discussion: This guideline was derived from Wagner et al. (1996), 6.10.2.1.7.

9.3.2-10 Interconnectivity

The number of inputs and outputs associated with a module should be minimized, where possible, to reduce the likelihood of errors in installing connections or testing multiple inputs and outputs.

Discussion: This guideline was derived from Wagner et al. (1996), 6.3.1.6.

9.3.2-11 Modularization Method

The modularization of digital equipment should be based on a systematic method that can be readily understood by maintenance personnel.

ADDITIONAL INFORMATION: Modularization, dividing a unit of equipment into individual modules, is a design strategy for enhancing maintainability. The following lists modularization methods that were recommended for the commercial aviation industry, in order of preference: (1) logical flow packaging, (2) circuit packaging, and (3) component packaging. In logical flow packaging, circuits, parts, and components are packaged and arranged in correspondence with their functional relationships. In circuit packaging, all parts of a single circuit or logically related group of parts, and only that circuit or group, are placed in a separate module. In component packaging, similar parts or components are located together, for example, all the fuses or all the relays might be grouped together.

Discussion: This guideline was derived from Wagner et al. (1996), 6.10.2.2.1. This guideline is also consistent with the high-level HSI design review principle, Logical/Explicit Structure, of NUREG-0700, Rev. 1 (See Appendix A).

9.3.2.1 Logical Flow Packaging

9.3.2.1-1 Isolating Module Faults via Single Input-Output Checks

When logical flow packaging is used to modularize digital equipment, a module should be designed so that only single input and output checks are necessary to isolate a fault in it.

Discussion: This guideline was derived from Wagner et al. (1996), 6.10.2.2.2.b.

9.3.2.1-2 Indication of Unidirectional Signal Flow

When logical flow packaging is used to modularize digital equipment, the unidirectional signal flow within a module should be clearly indicated.

Discussion: This guideline was derived from Wagner et al. (1996), 6.10.2.2.2.c.

9.3.2.2 Circuit Packaging

9.3.2.2-1 Locating Parts in a Single Module

When circuit packaging is used to modularize digital equipment, all parts of a given circuit or group of logically related parts should be located in a single module to help personnel find and test them.

ADDITIONAL INFORMATION: Testing and diagnosis may be difficult if related parts are distributed in many locations.

Discussion: This guideline was derived from Wagner et al. (1996), 6.10.2.2.3.a. It is also consistent with the high-level HSI design review principle, Logical/Explicit Structure, of NUREG-0700, Rev. 1 (see Appendix A).

9.3.2.2-2 Only One Circuit or Group of Related Parts Per Module

When circuit packaging is used to modularize digital equipment, a module should contain only one circuit or group of related parts to support testing and diagnosis.

ADDITIONAL INFORMATION: If a module contains multiple circuits or groups, then testing and diagnosis may be difficult (e.g., personnel may access the wrong parts when testing a circuit.)

Discussion: This guideline was derived from Wagner et al. (1996), 6.10.2.2.3.b. It is also consistent with the high-level HSI design review principle, Logical/Explicit Structure, of NUREG-0700, Rev. 1 (see Appendix A).

9.3.2.2-3 Packaging a Circuit as a Single Terminal-Board or Plug-In Module

When circuit packaging is used to modularize digital equipment, the circuit should be packaged as a single terminal board or plug-in module, when possible, to support its testing and installation.

ADDITIONAL INFORMATION: Providing a single board or module reduces the number of parts that must be handled and reduces the likelihood of errors during handling, testing, and installation.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.2.2.3.c.

9.3.2.2-4 Grouping Circuits to Minimize the Crossing of Signals
When circuit packaging is used to modularize digital equipment, circuits should be grouped to minimize criss-crossing of signals among modules.
ADDITIONAL INFORMATION: When circuits are improperly grouped, crossed signals may result from handling errors. Also, crossed signals can complicate fault detection and diagnosis.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.2.2.3.d.

9.3.2.3 Component Packaging

9.3.2.3-1 Grouping Components with Similar Replacement Schedule
When using component packaging to modularize digital equipment, similar parts that are likely to require replacement at approximately the same time should be grouped together.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.2.2.4.c.

9.3.2.3-2 Grouping Components with Similar Servicing Requirements
When component packaging is used to modularize digital equipment, components requiring the same maintenance work should be grouped together, e.g., test points or components requiring a particular cleaning method.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.2.2.4.d.

9.3.2.4 Printed Circuit Boards

9.3.2.4-1 Design for Removal and Replacement
Printed circuit boards should be designed and mounted for ease of removal and the elimination of errors during replacement.
ADDITIONAL INFORMATION: The physical design should make it impossible to install a printed circuit board upside down or backwards.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.2.2.5.a.

9.3.2.4-2 Plug-In Printed Circuit Boards
Plug-in printed circuit boards should be structurally rigid and easy to remove and replace, providing finger access and gripping aids if necessary.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.2.2.5.b.

9.3.2.4-3 Feedback When Installing Plug-In Printed Circuit Boards
Feedback should be provided to the maintainer when plug-in printed circuit boards are securely connected.
ADDITIONAL INFORMATION: For example, a tactile or audible "click" may indicate that the printed circuit board has been properly inserted.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.2.2.5.c.

9.3.2.4-4 Identification of Printed Circuit Boards and Parts
Printed circuit boards should be marked to identify the board and the parts mounted on it.
ADDITIONAL INFORMATION: MIL-STD-130J (U.S. Department of Defense, 1997) has guidance for identifying printed circuit boards. MIL-STD-454 (U.S. Department of Defense, 1985) Requirement 67, gives guidance on providing references for parts mounted on a printed circuit board.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.2.2.5.d.

9.3.3 Layout

9.3.3.1 Module Accessibility

9.3.3.1-1 No Interference from Other Parts

Modules should be laid out so that all parts can be removed and replaced without interference from or removal of other parts.
ADDITIONAL INFORMATION: Units that may have to be removed for maintenance should be situated so they can be moved without interference in straight horizontal or vertical paths.
Discussion: This guideline was derived from guideline 6.10.3.1.1 of Wagner et al. (1996). Additional information was derived from the second accessibility recommendation in Section IV A 2.1 of Pack et al. (1985).

9.3.3.1-2 No Stacking of Parts

To support accessibility, parts that make up a module should be mounted in an orderly, flat, two-dimensional array and should not be stacked one on top of another.
ADDITIONAL INFORMATION: An orderly, two-dimensional array allows parts to be accessed individually. Stacking is not recommended because some parts must be removed to provide access to the parts located below or behind them.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.3.1.2.

9.3.3.1-3 Consistent Orientation

If a module has more than one part of the same type that must be inserted in a particular orientation, all such parts should be oriented in the same direction.
ADDITIONAL INFORMATION: For example, a set of connectors should be installed with the same orientation.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.3.1.3.

9.3.3.1-4 Spacing of Parts

The parts that make up a module should be spaced and oriented so that required tools can be used without difficulty.
ADDITIONAL INFORMATION: For example, the spaces between parts should accommodate the use of test probes or soldering irons. Parts should be oriented so they can be reached with the required tools.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.3.1.4.

9.3.3.1-5 Separation of Parts and Wiring on Printed Circuit Boards

To support accessibility for testing parts on printed circuit boards, all parts should be mounted on one side of the board and all wiring, including printed circuits, should be located on the other side.
ADDITIONAL INFORMATION: Damage to circuit boards during testing can be avoided by making parts accessible.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.3.1.5.

9.3.3.1-6 Spacing of Terminals

Terminals to which wires are to be soldered should be far enough apart so that work on one terminal does not damage neighboring terminals or nearby parts.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.3.1.6.

9.3.3.1-7 Indicator Lights

If a module has indicator lights, it should be possible to change them from the front panel, without opening or removing the module.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.3.1.9.

9.3.3.1-8 Shutoff Switches

If the module contains emergency shutoff switches, they should be positioned within easy reach, and they should be located or guarded to prevent inadvertent operation.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.3.1.10.

9.3.3.1-9 Test, Adjustment, and Connection Points

Test points, adjustment points, and cable and line connectors should be located where the maintainer can see them easily and operate on them without interference.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.3.1.11.

9.3.3.2 Grouping

9.3.3.2-1 Grouping Maintenance Display Devices

All maintenance display devices relevant to a particular task should be grouped together and located where they can easily be seen.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.3.2.1.

9.3.3.2-2 Separate Maintenance and Operational Display Devices

If a unit of equipment contains both maintenance and operational display devices, the two types of devices should be separated.
Discussion: This was derived from guideline 6.10.3.2.2 of Wagner et al. (1996) and guideline 1.5.3.2.e of Bongarra et al. (1985). The Wagner et al. (1996) guideline states, "If a *module* contains both maintenance and operational *displays* ...". Wagner et al. (1996) cites as the basis for this guideline, Bongarra et al. (1985), 1.5.3.2.e which states, "If maintenance and operator displays must be located on the operator's panel, maintenance displays should be separated and grouped away from operator displays."

9.3.3.2-3 Separate Maintenance and Operational Displays in a Display Network

If a display device contains displays for both maintenance and operations personnel, then the maintenance displays should have a separate location in the display network.
ADDITIONAL INFORMATION: Maintenance displays should not be located within the same part of the display network as operational displays because their presence may interfere with the ability of operators to promptly access operational displays. Displays used by maintenance personnel generally should not be accessible by operational personnel, unless operators need them to perform their tasks. Access to maintenance displays should be protected by passwords, key locks, or similar measures.
Discussion: This guideline was derived from NUREG-1242 (NRC, 1994), 3.7.7; Wagner et al. (1996), 6.10.3.2.2; and Bongarra et al. (1985), 1.5.3.2.e. The concept of physical display devices addressed by these guidelines has been extended to computer-based displays in a display network.

9.3.4 Mounting

9.3.4-1 Prevention of Damage with Foldout Mounting

If foldout mounting is used, parts and wiring should be positioned so that they are not damaged during opening and closing.
ADDITIONAL INFORMATION: Figure 9.1 is an example of foldout mounting.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.4.2.

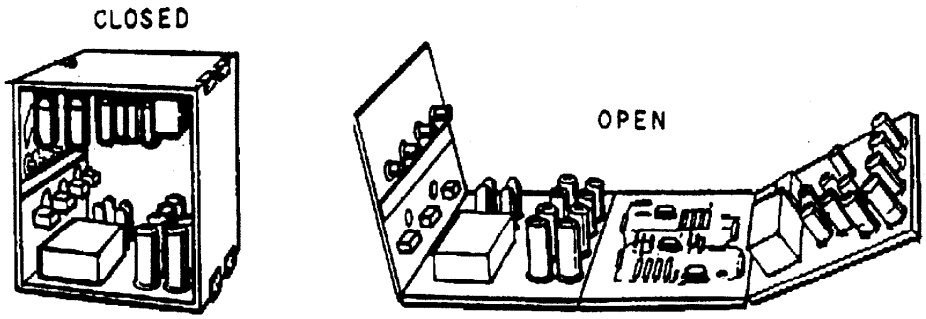

Figure 9.1 Example of Foldout Mounting Construction

9.3.4-2 Support for Hinged Mounting
If a module is mounted on hinges, supports should hold the module in the "out" or "open" position.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.4.3.

9.3.4-3 Rests and Stands
If a module contains parts that might be damaged when it is moved into position for maintenance, it should include rests or stands that are integral with the construction of the module to protect those parts.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.4.4.

9.3.4-4 Preventing Mounting Errors by Physical Design
Modules should be designed so that it is physically impossible to mount them incorrectly.
ADDITIONAL INFORMATION: Incorrect mounting includes reversal, mismating, and misaligning. Measures to prevent incorrect mounting include (1) incorporating keys or other aligning devices, (2) using asymmetrical mounting brackets, and (3) having asymmetrical mounting holes.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.4.7.

9.3.4-5 Controls
Modules should be mounted so that it is unnecessary to disconnect controls that may be needed for maintenance.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.4.10.

9.3.4-6 Front Access
Replaceable modules should be accessible through the front of the equipment, rather than the back, if the panel or console is not used by operators.
ADDITIONAL INFORMATION: Convenient access can reduce the likelihood of damage during installation, replacement, and testing. However, if maintenance is to be performed on-line, then access to the module access should not interfere with plant operations.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.4.12.

9.3.4-7 Orientation of Modules within Cases
If a module has a case, the proper orientation of the module within its case should be obvious, preferably through the physical design of the case, rather than through labeling.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.4.13.

9.3.4-8 Connectors

Electrical connections between modules should be simple and minimize the demands for manual dexterity.
ADDITIONAL INFORMATION: A plug-in connector requires minimal dexterity. Connectors requiring greater dexterity may be used when there are special requirements, such as holding power or sealing.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.4.14.

9.3.4-9 Standard Connectors

Connectors should be standardized as much as possible.
ADDITIONAL INFORMATION: Standardization reduces the need for different techniques for using each connector and may reduce the likelihood of errors from using the wrong technique.
Discussion: This guideline was derived from NUREG-1242 (NRC, 1994), 3.8.3.

9.4 Fuses and Circuit Breakers

9.4-1 Location of Fuses and Circuit Breakers

Fuses and circuit breakers should be grouped in a minimum number of centralized, readily accessible locations for removal, replacement, and resetting.
ADDITIONAL INFORMATION: Fuses should be located so they can be replaced without removing any other components.
Discussion: This guideline was derived from Wagner et al. (1996), 6.13.2.6 and 6.13.1.2.

9.4-2 Verification of an Open Circuit

An indication should be given when a fuse or circuit breaker has opened a circuit.
Discussion: This guideline was derived from Wagner et al. (1996), 6.13.1.3.

9.4-3 Individual Fused Units

Fuses or circuit breakers should be provided so that each unit of a system is separately fused and adequately protected from harmful variations in voltages that personnel may cause.
Discussion: This guideline was derived from Wagner et al. (1996), 6.13.1.4.

9.4-4 Worker Safety

Fuse installations should be designed so that only the neutral ("cold") terminal of the fuse can be touched.
ADDITIONAL INFORMATION: Shocks received from equipment may injure maintenance workers or cause them to make sudden movements, which can damage equipment.
Discussion: This guideline was derived from Wagner et al. (1996), 6.13.2.2.

9.4-5 Safeguarding the Circuit

Fuses should be provided that safeguard the circuit if the wrong switch or jack position is used.
Discussion: This guideline was derived from Wagner et al. (1996), 6.13.2.3.

9.4-6 Easily Removed Fuse Holders

Fuse holder cups or caps should be easily removed by hand.
ADDITIONAL INFORMATION: Fuse holder cups or caps should be of the quick-disconnect type rather than the screw-in type; they should be knurled and large enough to be handled easily. Replacing fuses should not require special tools, unless they are needed for safety.
Discussion: This guideline was derived from Wagner et al. (1996), 6.13.2.4.

9.4-7 Identifying Fuses and Circuit Breakers

Fuses and circuit breakers should be permanently labeled or marked.

ADDITIONAL INFORMATION: The labeling or marking should be legible in the anticipated ambient work conditions. Both fuses and fuse holders should be labeled.
Discussion: This guideline was derived from Wagner et al. (1996), 6.13.5.1. Guidance for labeling fuse holders was added based on industry experience.

9.4-8 Indicating Fuse Ratings

A fuse's rating should be indicated on the fuse and adjacent to the fuse holder.
ADDITIONAL INFORMATION: The rating should be in whole numbers, common fractions, such as ½, or whole numbers and common fractions, such as 2 ½.
Discussion: This guideline was derived from Wagner et al. (1996), 6.13.5.2. Guidance for labeling the fuse was based on industry experience.

9.4-9 Identifying Affected Circuits

The area of equipment served by a fuse or circuit breaker should be identified.
Discussion: This guideline was derived from Wagner et al. (1996), 6.13.5.3.

9.5 Labeling and Marking

9.5-1 Standard Labels

Equipment labels should be standardized as much as possible.
Discussion: This guideline was derived from NUREG-1242 (NRC, 1994), 3.8.3.

9.5-2 Information Content of Labels and Markings for Modules

Modules should be labeled or marked to supply information needed by maintainers.
ADDITIONAL INFORMATION: Labels or markings used for modules should

- outline and identify functional groups of parts
- identify each part by name or symbol
- indicate direction of current or signal flow to aid troubleshooting
- identify the value and tolerance level of parts or test points, if applicable
- identify each part by a unique serial identification number

Discussion: This guideline was derived from Wagner et al. (1996), 6.10.5.1. The requirements for a unique serial identification number were added based on industry experience.

9.5-3 Visibility of Labels and Markings

Labels and markings on parts or in cabinets should be placed so that the maintainer can see them without having to move or remove anything.
ADDITIONAL INFORMATION: The maintainer should not be required to remove parts or move wires to read labels and markings.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.5.4.

9.5-4 Consistent Placement of Labels and Markings

Labels and markings should be consistently placed in relation to the parts to which they refer.
ADDITIONAL INFORMATION: This placement may be on, or immediately adjacent to, the part.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.5.2.

9.5-5 Luminescent Labels

If labels must be read under very low ambient light, they may be marked in phosphorescent colors.
Discussion: This guideline was derived from Wagner et al. (1996), 6.14.6.6.

9.5-6 Electrical Parts

Small electrical parts that are attached to mounting boards, such as resistors and capacitors, should be labeled or marked on the mounting boards.
ADDITIONAL INFORMATION: Labeling and marking should appear on the mounting boards if the parts are too small to accommodate legible, salient labels and markings.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.5.6.

9.5-7 Identification of Parts
Parts should be identified with labels or markings.
ADDITIONAL INFORMATION: Labels or markings should be placed on either the parts themselves or on the chassis or adjacent board. The following types of parts that should be labeled or marked:
- All parts identified by designations in drawings, schematics, and parts descriptions of the module
- All wires, sockets, plugs, receptacles, and similar parts designated in wiring diagrams of the module
- All replaceable mechanical parts
- All semi-fixed electrical items, such as fuses and ferrule-clipped resistors
- Items having critical polarity or impedance ratings

Discussion: This guideline was derived from Wagner et al. (1996), 6.10.5.7.

9.5-8 Identification of Terminals on Terminal Strips or Blocks
The terminals of terminal strips or blocks should be labeled on the strip or block, or on the chassis, adjacent to the terminals.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.5.8.

9.5-9 Identification of Terminals on Parts
When parts have terminals (e.g., transformers, relays, and capacitors), each terminal should be identified by an adjacent label.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.5.9.

9.5-10 Identification of Parts Accessible from Both Sides
Receptacles that are accessible from both sides of a board or panel should be identified on both sides.
ADDITIONAL INFORMATION: Some boards and panels contain receptacles that allow parts to be accessed from either side.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.5.10.

9.5-11 Durability of Markings
Markings should be durable enough to last the life of the equipment.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.5.12.

9.5-12 Marking Stacked Parts
If parts or modules are stacked, marking should permit identification of the individual parts or modules.
ADDITIONAL INFORMATION: Stacking of parts or modules is not recommended (see guideline 9.3.3.1-2).
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.5.13.

9.5-13 Marking Enclosed or Shielded Parts, Modules, Test Points, and Service Points
Enclosed or shielded parts, modules, test points, and service points should be marked both outside the enclosure or shield, and inside it.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.5.14 and 6.14.6.8.

9.5-14 Hazard Warnings

If there is any hazard from a part or module, a warning or caution label should be provided on it, on the case or cover, or both.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.5.16.

9.5-15 Labeling Symmetrical Parts
Parts that are symmetrical should be labeled or marked to indicate their proper orientation for mounting.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.5.17.

9.5-16 Insertion Holes
If a module has holes through which parts must be aligned and then inserted, labels showing the proper orientation of the part should be placed adjacent to the holes.
ADDITIONAL INFORMATION: Tubes and connectors are examples of parts that may be inserted through holes in modules.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.5.18.

9.5-17 Auxiliary Information for Parts
Parts to which auxiliary information applies should be labeled with that information.
ADDITIONAL INFORMATION: Examples of auxiliary information include values and tolerances of resistors and capacitors. This information should be in an easily readable form.
Discussion: This guideline was derived from Wagner et al. (1996), 6.10.5.19.

9.6 Adjustment Controls

9.6-1 Misalignment
Controls and displays should be designed to prevent misalignment that might be caused by vibration, service use, or accidental contact.
Discussion: This guideline was derived from Wagner et al. (1996), 6.15.1.4.4.

9.6-2 Controls and Feedback
Each adjustment control should provide feedback.
ADDITIONAL INFORMATION: This feedback might be visual, audible, or tactile.
Discussion: This guideline was derived from Wagner et al. (1996), 6.11.1.

9.6-3 Simultaneous Access to Controls and Displays
Maintainers should have simultaneous access to an adjustment control and its associated display or other source of feedback.
ADDITIONAL INFORMATION: Maintainers should be able to observe the effects of adjustments as they are made.
Discussion: This guideline was derived from Wagner et al. (1996), 6.11.2.

9.6-4 Differentiating Maintenance Controls from Operational Controls
Maintenance and operational controls should be clearly differentiated.
Discussion: This guideline was derived from Wagner et al. (1996), 6.11.4.

9.6-5 Location of Maintenance and Operational Controls
The maintenance and operational controls should not appear on the same panel if maintenance and operation of a unit of equipment are performed by different sets of people.
ADDITIONAL INFORMATION: If maintenance and operational controls must appear on the same panel, the maintenance controls should be grouped and separated from the operational controls. If appropriate, the

maintenance controls might also be guarded with removable covers so as not to interfere with the operator's performance.
Discussion: This guideline was derived from Wagner et al. (1996), 6.11.4 and NUREG-1242 (NRC, 1994), 3.7.7.

9.6-6 Independence of Adjustment Controls
Where possible and practical, the adjustment of one control should be independent of the adjustments of others.
Discussion: This guideline was derived from Wagner et al. (1996), 6.11.5.

9.6-7 Sequential Adjustments
If the adjustment of one control affects the adjustment of another, the controls should be arranged in sequential order, and labeled or marked to indicate the order of adjustment.
Discussion: This guideline was derived from Wagner et al. (1996), 6.11.6.

9.6-8 Functionally Related Adjustments
If a single control is used to affect multiple variables, then the user interface should be designed to prevent mode errors.
ADDITIONAL INFORMATION: Mode errors occur when the user performs an action that is appropriate for one mode when a different mode is in effect. Four design strategies for preventing mode errors are eliminating modes, making modes distinct, providing different inputs for different modes, and coordinating inputs across modes. Eliminating modes prevents mode errors by eliminating the conditions under which they occur (i.e., if there are no modes there can be no mode errors). Making modes distinct deals with the problem through feedback. By saliently indicating the currently active mode, operators are more likely to be aware of it and less likely to provide an incompatible input. Providing different inputs for different modes addresses the problem by ensuring that the same input is not valid in more than one mode. Thus, if the operator provides an input while in the wrong mode, the system will not accept it. Coordinating inputs across modes ensures that a command producing a benign effect in one mode does not produce a severely negative effect in another mode.
Discussion: This guideline was derived from Stubler, O'Hara, and Kramer (2000).

9.6-9 Degree of Adjustment
Controls should accommodate the degree of adjustment required; that is, gross adjustment, fine adjustment, or both.
Discussion: This guideline was derived from Wagner et al. (1996), 6.11.14.

9.6-10 Mechanical Stops
Adjustment controls intended to have a limited range of motion should have mechanical stops.
ADDITIONAL INFORMATION: These stops should be able to withstand a force or torque 100 times greater than the resistance to movement within the range of adjustment.
Discussion: This guideline was derived from Wagner et al. (1996), 6.11.15.

9.6-11 Previous Settings
If a task requires that a maintainer be able to quickly return a control to its previous setting, the control should have a scale and pointer, or equivalent.
Discussion: This guideline was derived from Wagner et al. (1996), 6.11.16.

9.6-12 Preventing Inadvertent Adjustment
Adjustment controls should be located and mounted so that they cannot be adjusted inadvertently.
Discussion: This guideline was derived from Wagner et al. (1996), 6.11.17.

9.6-13 Critical or Sensitive Adjustments

Critical or sensitive adjustments should incorporate features, such as locking devices, to prevent inadvertent or accidental adjustment.
ADDITIONAL INFORMATION: If a locking device is used, its operation should not change the adjustment setting.
Discussion: This guideline was derived from Wagner et al. (1996), 6.11.18.

9.6-14 Hand or Arm Support

If an adjustment control or the maintainer will be subject to vibration during adjustment, a suitable hand or arm support should be provided.
ADDITIONAL INFORMATION: Vibrations can cause the maintainer to overshoot or undershoot the desired adjustment value.
Discussion: This guideline was derived from Wagner et al. (1996), 6.11.19.

9.7 Test Points and Service Points

9.7.1 General

9.7.1-1 Ease of Servicing

Equipment should be designed so that it can be serviced in its installed position to prevent errors associated with disassembling and reassembling it.
Discussion: This guideline was derived from Wagner et al. (1996), 6.1.5.1.

9.7.1-2 Appropriate Use of Test Points

Test points should be provided on units of equipment as required to support personnel in checking, adjusting, and troubleshooting it.
ADDITIONAL INFORMATION: Strategically placed test points make signals available to maintenance personnel. Test points may not be required if the equipment has self-checking capabilities.
Discussion: This guideline was derived from the introductory discussion of Section 6.14, Test Points and Service Points, in Wagner et al. (1996).

9.7.1-3 Single Adjustment Control Per Test Point

A test point should not have more than one associated adjustment control.
Discussion: This guideline was derived from Wagner et al. (1996), 6.14.1.2.

9.7.1-4 Ground Points

Special grounding points should be provided, as needed, in locations in which surfaces have poor electrical grounding characteristics.
ADDITIONAL INFORMATION: Maintainers may have difficulty if only painted surfaces are available for ground connections.
Discussion: This guideline was derived from Wagner et al. (1996), 6.14.5.5.

9.7.2 Location, Arrangement, and Marking

9.7.2-1 Test Points for Units of Equipment

Where possible, each input to and output from a unit of equipment should have test points to support testing and diagnosis of faults.
Discussion: This guideline was derived from Wagner et al. (1996), 6.14.2.1.

9.7.2-2 Tracing Signals
Test points should be provided to permit the systematic tracing of signals and voltages through a unit of equipment to support fault detection and diagnosis.
ADDITIONAL INFORMATION: These test points allow a maintainer to determine the point at which signals or voltages in a malfunctioning unit are out of tolerance.
Discussion: This guideline was derived from Wagner et al. (1996), 6.14.2.3.

9.7.2-3 Test and Service Point Accessibility
All test and service points should be visible and physically accessible to the maintainer for checking and troubleshooting.
ADDITIONAL INFORMATION: Recommended minimum clearances are 19 mm (0.75 in) when only finger control is required, and 75 mm (3 in) when using gloves.
Discussion: This guideline was derived from Wagner et al. (1996), 6.14.4.1 and 6.14.2.4.

9.7.2-4 Proximity of Controls, Displays, and Test Points
Test points should be located in physical and visual proximity to the controls and displays used to make the adjustments.
ADDITIONAL INFORMATION: The adjustment control should provide a signal detectable at the test point that clearly indicates when the correct adjustment has been made.
Discussion: This guideline was derived from Wagner et al. (1996), 6.14.1.1 and 6.14.2.5.

9.7.2-5 Proximity of Controls, Displays, and Service Points
Service points should be located in physical and visual proximity to the controls and displays used when adjusting them.
Discussion: This guideline was derived from Wagner et al. (1996), 6.14.2.5.

9.7.2-6 Test and Service Point Location
Test and service points should be provided, designed, and located in accordance with their frequency of use and any time-limits on maintenance.
ADDITIONAL INFORMATION: Isolated test or service points should be avoided because they are likely to be overlooked or neglected.
Discussion: This guideline was derived from Wagner et al. (1996), 6.14.2.6 and 6.14.2.9.

9.7.2-7 Compatibility of Test and Service Points
Test and service points should be designed for compatibility with checking, troubleshooting, and servicing procedures, and with test and service equipment.
Discussion: This guideline was derived from Wagner et al. (1996), 6.14.2.10.

9.7.2-8 Distinctive Connections
Each type of test or service equipment should have distinctively different connectors or fittings to minimize the likelihood of error.
ADDITIONAL INFORMATION: Providing visually distinct connectors or fittings for different types of test and service equipment may reduce the likelihood that a maintainer will mistake one type for another. Physical differences between different types of connectors and fittings may prevent a maintainer from connecting the wrong piece of test or service equipment, if it is physically incompatible with the test or service connector or fitting.
Discussion: This guideline was derived from Wagner et al. (1996), 6.14.2.11.

9.7.2-9 Distinguishable Marking

Test and service points should be designed and marked so that they are easily distinguishable from each other.
ADDITIONAL INFORMATION: If color coding is used, the color of test points should clearly differ from that of service points.
Discussion: This guideline was derived from Wagner et al. (1996), 6.14.6.2.

9.7.3 Accessibility

9.7.3-1 Access Openings for Test Equipment
Access openings necessary to connect test equipment should accommodate maintainers, equipment, and required tools.
Discussion: This guideline was derived from Wagner et al. (1996), 6.15.1.3.1.

9.7.3-2 Test Probe Guides
Suitable guides for test probes should be provided when test points are located internally to an enclosure.
ADDITIONAL INFORMATION: When a maintainer inserts a test probe through an opening in an enclosure, a guide can help the test probe make contact with the internal test point.
Discussion: This guideline was derived from Wagner et al. (1996), 6.14.4.2.

9.8 Test Equipment

9.8.1 General

9.8.1-1 Built-In Test Capabilities
All test capabilities for a unit of equipment should be built in, to the extent feasible, to reduce the likelihood of testing errors.
ADDITIONAL INFORMATION: Built-in test capabilities can avoid errors associated with disassembling plant equipment or connecting test equipment. The handling involved with removing and transporting a component to a test site may introduce new faults in sensitive equipment. Built-in diagnostics and testing features allow equipment to be tested in place. If it is not practical or possible to incorporate all test equipment, then test jacks may be provided to allow internal components to be tested by external test devices without disassembling the plant equipment.
Discussion: This guideline was derived from NUREG-1242 (NRC, 1994), 6.2.2 and Bongarra et al. (1985), 1.7.4.1.c.(1 to 5).

9.8.1-2 Appropriate Use of Alarms
If critical equipment is not regularly monitored, an alarm should be provided to indicate malfunctions or conditions that would cause personnel injury or equipment damage.
ADDITIONAL INFORMATION: The alarm may be auditory, visual, or both. If an auditory alarm would be overly intrusive or disruptive, the alarm should be visual. A combination of auditory and visual alarms should be provided when the ambient illumination may impair the maintainer's ability to see the latter. A high degree of ambient illumination may cause visual glare, affecting the detection of light-emitting alarms. A low degree of ambient illumination may interfere with their ability to detect and read alarms on light-reflecting displays.
Discussion: This guideline was derived from Wagner et al. (1996), 6.12.1.1 , 6.12.1.2, and 6.12.1.3.

9.8.1-3 Accuracy of Test Equipment
The accuracy of test equipment should be consistent with testing requirements.

ADDITIONAL INFORMATION: In general, the accuracy of test equipment should exceed that of the equipment being tested.
Discussion: This guideline was derived from Wagner et al. (1996), 6.15.1.1.2.

9.8.1-4 Instructions
Clearly written and easily understandable operating instructions for the test equipment should be available to the maintainer.
Discussion: This guideline was derived from Bongarra et al. (1985), 1.8.3.2(c).

9.8.1-5 Labels
Equipment labels should identify all items the maintainer must be able to recognize, read, or use.
ADDITIONAL INFORMATION: The test equipment should be labeled to identify the equipment, its purpose, and any precautions that should be observed in its use. There should be adequate warnings wherever potential hazards exist.
Discussion: This guideline was derived from Wagner et al. (1996), 6.15.1.1.8. The additional information was derived from Wagner et al. (1996), 6.15.1.1.7 and 6.15.1.2.8.

9.8.1-6 Minimizing Errors
The test equipment should be designed to minimize the occurrence of errors by the maintainer.
ADDITIONAL INFORMATION: If possible, it should provide messages to support the detection of errors.
Discussion: This guideline was derived from Wagner et al. (1996), 6.15.1.2.4.

9.8.1-7 Minimizing Hazards
When possible, fail-safe features should be incorporated in test equipment to minimize dangers to maintainers or equipment.
ADDITIONAL INFORMATION: For example, test equipment should have fuses or other protective features to prevent damage or injury if a wrong switch or jack position is used.
Discussion: This guideline was derived from Wagner et al. (1996), 6.15.1.2.5. Additional information was derived from Wagner et al. (1996), 6.15.1.2.2.

9.8.2 Automatic Test Equipment

9.8.2-1 Automated Aids
Fault isolation, inspection, and checkout tasks should be automated to the extent practical to support personnel performance.
ADDITIONAL INFORMATION: These tasks are prone to human error. At a minimum, self-check diagnostic tests should operate automatically on power up of plant equipment and at the operator's request.
Discussion: This guideline was derived from Wagner et al. (1996), 6.12.3.1 and 6.12.3.2.

9.8.2-2 On-Line Diagnostics
Computer systems should have on-line diagnostic capabilities, if the detection and diagnosis of computer faults is required.
ADDITIONAL INFORMATION: The detection and diagnosis of computer faults can be complicated and difficult. On-line diagnostic capabilities, which allow computer systems to be tested while they are running, can be effective for finding faults because they test the computer under operating conditions. On-line diagnostic capabilities should be able to check both hardware and software when the symptoms may appear similar to maintenance personnel. Checks may be used to detect software malfunctions and unauthorized changes in software.
Discussion: This guideline was derived from NUREG-1242 (NRC, 1994), 6.1.4.

9.8.2.1 Test Intervals

9.8.2.1-1 Continuous On-Line Self-Testing

The capability for continuous on-line self-testing should be provided when practicable to support prompt detection of faults.

ADDITIONAL INFORMATION: Continuous on-line self-testing allows tests to be performed with minimal involvement by personnel, and can reduce the amount of time between the occurrence and the detection of a fault. Tests may include, but should not be limited to, random access memory and read-only memory failure checks, arithmetic processing unit failure checks, data link buffer checks, and central processing unit reset of watchdog timers. For safety-related systems, testing features should be designed to reduce the complexity of safety-related software logic and data structures.

Discussion: This guideline was derived from NUREG-1242 (NRC, 1994), 3.6.1.

9.8.2.1-2 Periodic Testing

The capability for periodic functional testing that is manually initiated but executed automatically should be provided when personnel require control of the test intervals.

ADDITIONAL INFORMATION: Automatic execution of tests is preferred when human errors may cause transients.

Discussion: This guideline was derived from NUREG-1242 (NRC, 1994), 3.6.2.

9.8.2.2 Bypasses for Plant and Test Equipment

9.8.2.2-1 Automatic Bypass

When a test is initiated manually, the correct bypasses required for testing should be established automatically, and the operators should be aware of all of them.

ADDITIONAL INFORMATION: When a component is tested, it may be necessary to bypass other systems or functions associated with the component to prevent them from being affected. The operators should be made aware of these bypasses.

Discussion: This guideline was derived from NUREG-1242 (NRC, 1994), 3.6.10 and reflects guidance from Regulatory Guide 1.47 (NRC, 1973).

9.8.2.2-2 Indicators for Test and Bypass Status

Local indication of pass or fail for test and bypass status should be provided for periodic functional tests.

ADDITIONAL INFORMATION: Indicators should be provided at the local cabinet to quickly show the pass or fail status for the test, and the status of bypasses.

Discussion: This guideline was derived from NUREG-1242 (NRC, 1994), 3.6.11.

9.8.2.2-3 Removal of Automatic Bypass

When a periodic functional test sequence is completed, all bypasses established to allow the test to be performed should be automatically removed, to relieve the operator of this task.

ADDITIONAL INFORMATION: Indications should be given to allow operators to verify the status of the bypasses and that the system has been properly reconfigured for normal operation. Removal of automatic bypasses may reduce the potential for errors which could unintentionally activate equipment.

Discussion: This guideline was derived from NUREG-1242 (NRC, 1994), 3.6.13 and reflects guidance from Regulatory Guide 1.47 (NRC, 1973).

9.8.2.2-4 Bypassed Diagnosis Routines

To support the diagnosis of faults, diagnosis routines that are bypassed during maintenance should be run again before equipment is put back in service.

ADDITIONAL INFORMATION: When a component is serviced, it may be necessary to disable some automatic diagnosis routines. Running the routines before the equipment is put back into service ensures that they are available. It also supports the detection of any faults that may have occurred during testing. Failure to restore the diagnostic routines may increase the time required to detect future faults.
Discussion: This guideline was derived from NUREG-1242 (NRC, 1994), 6.1.3.15.

9.8.2.3 Failure Indications

9.8.2.3-1 Loss of Redundancy

If part of a redundant system, unit of equipment, module, or component becomes inoperable, an alarm signaling the loss of redundancy should be provided to the user immediately.
ADDITIONAL INFORMATION: Users should be able to acknowledge such an alarm, but the lack of available redundancy should be continuously displayed until the redundant system, equipment, module, or component becomes operable again.
Discussion: This guideline was derived from Wagner et al. (1996), 6.12.1.4 and reflects guidance from Regulatory Guide 1.47 (NRC, 1973).

9.8.2.3-2 Overload Indications

Overload indications should be provided for equipment subject to this condition.
ADDITIONAL INFORMATION: This indication should be provided even if the equipment continues to operate when overloaded.
Discussion: This guideline was derived from Wagner et al. (1996), 6.12.2.1.

9.8.2.3-3 Identification of In-Tolerance Ranges

When practical, the ranges for which test values are within acceptable tolerance limits should be indicated on built-in test equipment.
ADDITIONAL INFORMATION: For example, an in-tolerance reading for a meter or an in-tolerance wave shape for an oscilloscope should be coded for each position of the rotary switch of the built-in test equipment.
Discussion: This guideline was derived from Bongarra et al. (1985), 1.7.4.1.c.1.

9.8.2.3-4 Out-of-Range Indicators

If equipment has failed or is not operating within tolerance limits, an indication should be provided.
Discussion: This guideline was derived from Wagner et al. (1996), 6.12.2.2.

9.8.2.3-5 Power Failure Indicators

If a power failure occurs, an indication should be given.
Discussion: This guideline was derived from Wagner et al. (1996), 6.12.2.3.

9.8.2.3-6 Open Circuit Indicators

If a fuse or circuit breaker has opened a circuit, there should be an indication.
Discussion: This guideline was derived from Wagner et al. (1996), 6.12.2.4.

9.8.2.3-7 Power-On Indicator

A power-on indicator that extinguishes with loss of power should be provided.
Discussion: This guideline was derived from Wagner et al. (1996), 6.12.2.5.

9.8.2.4 Display of Test Results

9.8.2.4.-1 Inclusion of Fault Messages

Fault messages should only be shown if they add value to the maintenance process.
ADDITIONAL INFORMATION: The presence of unnecessary fault messages can reduce the effectiveness of maintenance personnel by increasing the workload associated with locating and using messages that support diagnosis and repair. The flexibility of computer-based technologies and the needs of secondary users of the maintenance system can result in the inclusion of variables and capabilities that do not support the performance of primary users. Limiting messages to those that are valuable to the maintenance process can help personnel use the automated test equipment effectively. The status of some variables can be determined by direct observation without using automated test equipment. The appropriateness of including these variables in a test device should be based on consideration of their effects on maintenance performance. Thus, the burdens associated with viewing additional variables should be weighed against the potential benefits of having fault indications consolidated in a test device.
Discussion: This guideline is based on a review of problems that have been encountered with built-in test systems used in commercial aircraft maintenance (Hessburg, 1992). It is also consistent with the high-level HSI design review principle, Simplicity of Design, of NUREG-0700, Rev. 1, which states, "The HSI should represent the simplest design consistent with functional and task requirements" (O'Hara, Brown, Stubler, Wachtel, and Persensky, 1996, p. A-2; see Appendix A).

9.8.2.4-2 Direct Interpretation of Test Results
Messages provided by test equipment should require a minimum amount of interpretation.
ADDITIONAL INFORMATION: Messages provided by test equipment should not use abbreviations, contractions, or numeric codes. Conversion tables should not be needed to determine whether the equipment is within tolerances. Test equipment that requires maintenance personnel to read codes and then look up the code on a table to obtain an explanation are susceptible to errors in reading, recording, and looking up the codes.
Discussion: This guideline is based on Wagner et al. (1996), 6.15.1.1.3, which states that conversion tables should not be used in deciding if equipment is within tolerances. This guideline is also based on a review of problems that have been encountered with built-in test systems used in commercial aircraft maintenance, especially difficulties in interpreting messages that have abbreviations and contractions (Hessburg, 1992). It is consistent with the high-level HSI design review principle, Task Compatibility, of NUREG-0700, Rev. 1 (see Appendix A).

9.8.2.4-3 Identification of Failure Location
Test features should identify the location of the detected failure to the lowest replaceable module.
ADDITIONAL INFORMATION: Test equipment should also inform maintenance personnel of the types of actions required to return the equipment to service. For example, even though the failure exists in component A, the corrective action may require that components B, C, and D are replaced at the same time.
Discussion: This guideline was derived from NUREG-1242 (NRC, 1994), 3.6.5. Additional information was based on a review of problems that have been encountered with BIT systems used in commercial aircraft maintenance (Hessburg, 1992).

9.8.2.4-4 Identification of Out-of-Tolerance Signals on Collating Test Equipment
If equipment fails a test performed by collating test equipment, the test equipment should indicate which signal(s) are out of tolerance.
ADDITIONAL INFORMATION: Collating test equipment presents the results of two or more checks as a single display; for example, a "test passed" light illuminates only if all of the relevant signals are within tolerance. Collating test equipment reduces the number of displays the maintainer must read, thereby reducing testing time. However, it should identify the out-of-tolerance signal(s) rather than merely indicating that the equipment failed the test.
Discussion: This guideline was derived from Wagner et al. (1996), 6.15.5.1. The additional information was derived from Wagner et al. (1996), 6.15.5.

9.8.3 Test Equipment Hardware

9.8.3.1 General

9.8.3.1-1 Requirements for Test Equipment and Bench Mockups
Test equipment and bench mockups should be treated like any other equipment with respect to the HFE design requirements for units, covers, cases, cables, connectors, test points, displays, and controls.
ADDITIONAL INFORMATION: Test equipment and bench mockups should be designed to be consistent with the capabilities of users and to prevent personal injury.
Discussion: This guideline was derived from Wagner et al. (1996), 6.15.1.1.1.

9.8.3.1-2 Selector Switches
Selector switches should be used rather than many, individual plug-in connections as long as the effects of switching do not degrade the desired information.
ADDITIONAL INFORMATION: When connecting test equipment to particular circuits, selector switches can be used more quickly than many, individual plug-in connections, and can reduce the likelihood of incorrect or faulty connections.
Discussion: This guideline was derived from Wagner et al. (1996), 6.15.1.1.4.

9.8.3.1-3 Minimizing Test Equipment Accessories
The number and types of test equipment accessories, such as connectors and test cables, should be minimized.
Discussion: This guideline was derived from Wagner et al. (1996), 6.15.1.3.2.

9.8.3.1-4 Minimizing Test Equipment Controls, Displays, and Modes
Test equipment should be simple to operate and have a minimum number of controls, displays, and modes.
ADDITIONAL INFORMATION: Controls and displayed information should be organized to reduce the amount of mental effort required to find, access, and use them. Test equipment should not have many individual control and display devices that the maintainer must coordinate to operate it. However, their number should not be reduced to such a degree that many control and display modes are introduced, which can create opportunities for mode errors.
Discussion: This guideline was derived from Bongarra et al. (1985), 1.8.3.2(a), which states that the number of controls and displays should be kept to a minimum, and Wagner et al. (1996), 6.15.1.3.3, which states that test equipment should be simple to operate and have a minimum number of controls and displays.

9.8.3.1-5 Reducing the Number and Complexity of Steps
The number and complexity of steps required to operate the test equipment should be minimized.
ADDITIONAL INFORMATION: The number and complexity of steps may be reduced by grouping controls, such as by sequence or criticality, or by automating certain operations.
Discussion: This guideline was derived from Bongarra et al. (1985), 1.8.3.2. The additional information was derived from Wagner et al. (1996), 6.15.1.3.4.

9.8.3.1-6 Individual Operation
Test equipment should be designed for operation by one person, if practical.
Discussion: This guideline was derived from Wagner et al. (1996), 6.15.1.3.5.

9.8.3.1-7 Calibration Check
Test equipment should be easily calibrated or equipped with a simple check to indicate whether or not it is out-of-calibration or malfunctioning.

ADDITIONAL INFORMATION: A go/no-go indicator may provide a simple check of the status of the test equipment.
Discussion: This guideline was derived from Wagner et al. (1996), 6.15.1.4.1.

9.8.3.1-8 Avoid Temporary Equipment Configurations for Testing
The use of temporary equipment configurations for periodic, functional testing of equipment should be avoided.
ADDITIONAL INFORMATION: Temporary equipment configurations include added jumpers, lifting leads, and swapping cables. Built-in test features may alleviate problems experienced in NPPs that result from designs with poor testability.
Discussion: This guideline was derived from EPRI (1993), 3.6.1.

9.8.3.2 Portable Test Equipment

9.8.3.2-1 Portable Diagnostic Tools
Portable diagnostic equipment should be provided to aid in fault isolation when built-in equipment is not practical.
ADDITIONAL INFORMATION: Built-in equipment is generally preferable to portable equipment when it eliminates activities prone to error, such as disassembling plant equipment or connecting portable test equipment.
Discussion: This guideline was derived from Wagner et al. (1996), 6.12.3.9.

9.8.3.2-2 Ease of Connection
Portable test equipment should allow rapid and error-free connection to the equipment being tested.
ADDITIONAL INFORMATION: The use of a single, multi-prong connector can avoid errors that could occur if multiple wires were connected individually.
Discussion: This guideline was derived from Wagner et al. (1996), 6.15.2.3.2.

9.8.3.2-3 Calibration Information
If maintenance personnel are required to verify that test equipment has been calibrated, then this information should be available to them.
ADDITIONAL INFORMATION: A calibration record may be attached to the equipment with this information.
Discussion: This guideline was derived from Wagner et al. (1996), 6.15.2.3.5.

9.3.8.3 Built-In Test Panel

9.3.8.3-1 Test Point Connections
Test points should permit the connection of the appropriate test equipment, such as voltage meters.
ADDITIONAL INFORMATION: The purpose of a built-in test panel is to allow external test devices to assess internal components without disassembling the plant equipment.
Discussion: This guideline was derived from Wagner et al. (1996), 6.15.2.4.2.

9.3.8.3-2 Test Point Indication Labeling and Demarcation
Test points should be clearly indicated on the test panel.
ADDITIONAL INFORMATION: For example, test points might be arranged within a miniature block diagram of the system with each block representing components or units of equipment. As another example, an overlay may be provided to indicate the test points that should be checked, the order in which they should be checked, and the tolerance limits for signals.
Discussion: This guideline was derived from Wagner et al. (1996), 6.15.2.4.3, 6.15.2.4.4, and 6.15.2.4.4.

APPENDIX A

High-Level Design Review Principles From NUREG-0700, Rev. 1

NUREG-0700 HIGH-LEVEL DESIGN REVIEW PRINCIPLES

The design of human-system interfaces (HSIs) should support the operating personnel's primary task of monitoring and controlling the plant, without imposing an excessive workload associated with using them (manipulating windows, selecting display selection, and navigating, for example). The HSI also should support the recognition, tolerance, and recovery from human errors. Guidelines for reviewing human factors engineering design help to ensure that these goals are achieved. As part of the guidance development for NUREG-0700, Rev. 1, a set of "high-level" design review principles were established representing the generic HSI characteristics necessary to support personnel's performance. They were used to draft many detailed review guidelines in Part 2 of NUREG-0700 (see O'Hara, Brown, and Nasta, 1996 for a discussion of their use). The high-level principles also were used in the formulating guidelines for computer-based procedures.

The 18 principles are divided into four categories: general principles, primary task design, secondary task control, and task support . The categories and the principles that comprise them are described below.

General Principles

These principles ensure that the HSI design supports personnel safety, and is compatible with people's general cognitive and physiological capabilities.

Personnel Safety – The design should minimize the potential for injury and exposure to harmful materials.

Cognitive Compatibility – The operators' role should consist of purposeful, meaningful tasks that enable them to remain familiar with the plant, and maintain a level of workload that is not so high as to negatively affect performance, but sufficient to maintain vigilance.

Physiological Compatibility – The design of the interface should reflect physiological characteristics, including visual and auditory perception, biomechanics (reach and motion), motor control, and anthropometry.

Simplicity of Design – The HSI should represent the simplest design consistent with functional and task requirements.

Consistency – There should be a high degree of consistency between the HSI, the procedures, and the training systems. At the HSI, the way the system functions and appears to the operating crew always should reflect a high degree of standardization, and consistency with procedures and training.

Primary Task Design

These principles support the operator's primary task of process monitoring, decision making, and control to maintain safe operation.

Situation Awareness – The information presented to the users by the HSI should be correct, rapidly recognized, and easily understood (e.g., "direct perception" or "status-at-a-glance" displays) and support the higher-level goal of user's awareness of the system's status.

Task Compatibility – The system should meet the requirements of users to perform their tasks (including operation, safe shutdown, inspection, maintenance, and repair). The forms and formats of data should be appropriate to the task (including the need to access confirmatory data or raw data in the

case of higher-level displays), and control options should encompass the range of potential actions. No unnecessary information or control options should be present.

User Model Compatibility – All aspects of the system should be consistent with the users' mental models (understanding and expectations about how the system behaves, learned through training, using procedures, and experience). All aspects of the system also should be consistent with established conventions (i.e., expressed in customary, commonplace, useful, and functional terms, rather than abstract, unusual or arbitrary forms, or in forms requiring interpretation).

Organization of HSI Elements – The organization of all aspects of the HSI (from the elements in individual displays, to individual workstations, to the entire control room) should be based on the user's requirements and should reflect the general principles of organization by importance, frequency, and order of use. Critical safety function information should be available to the entire operating crew in dedicated locations to ensure its recognition, and to minimize data search and response.

Logical/Explicit Structure – All aspects of the system (formats, terminology, sequencing, grouping, and the operator's decision-support aids) should reflect an obvious logic based on task requirements or some other non-arbitrary rationale. There should be a clear relationship of each display, control, and data-processing aid to the overall task or function. The structure of the interface and its associated navigation aids should make it easy for users to recognize where they are in the data space, and enable them to rapidly access data not currently visible (e.g., on other display pages). The way the system works and is structured should be clear to the user.

Timeliness – The system's design should take into account users' cognitive processing capabilities as well as process-related time constraints to ensure that tasks can be performed within the time required. Information-flow rates and control-performance requirements that are too fast or too slow could diminish performance.

Controls/Displays Compatibility – Displays should be compatible with the requirements for data entry and control.

Feedback – The system should provide useful information on its status, permissible operations, errors and error recovery, dangerous operations, and validity of data.

Secondary Task Control

These principles minimize secondary tasks, i.e., tasks personnel must perform when working with the system that are not directed to the primary task. Secondary tasks include managing the interface, such as navigating through displays, manipulating windows, and accessing data. Performing secondary tasks detracts from the crew's primary tasks, so their demands must be controlled.

Cognitive Workload – The information presented by the system should be rapidly recognized and understood; therefore, its design should minimize the need for mental calculations or transformations, and use of recall memory (recalling lengthy lists of codes, complex command strings, information from one display to another, or lengthy action sequences). Raw data should be processed into a directly usable form (although raw data still should be accessible for confirmation).

Response Workload – The system should require a minimum number of steps to accomplish an action, e.g., single-versus command-keying, menu selection versus multiple-command entry, single input mode (keyboard, mouse) versus mixed mode. In addition, it should not require the entry of redundant

data, nor the re-entry of information already present, or information the system can generate from data already resident.

Task Support

These principles address the characteristics of the HSI that support its use by personnel, such as providing (1) HSI flexibility so tasks can be accomplished in more than one way, (2) guidance for users, and (3) mitigation of errors.

Flexibility – The system should give the user multiple means to carry out actions (and verify automatic actions), and permit displays and controls to be configured in the most convenient way. However, flexibility should be limited to situations where it is advantageous in task performance (e.g., in accommodating different levels of experience of the users); flexibility should not be provided for its own sake because there is a tradeoff between consistency and the imposition of interface management workload (which detracts from monitoring and operations).

User Guidance and Support – The system should provide an effective "help" function; i.e., informative, easy-to-use, and relevant guidance should be provided on-line and off-line to help the user understand and operate the system.

Error Tolerance and Control – A fail-safe design should be provided wherever failure can damage equipment, injure personnel, or inadvertently operate critical equipment. Therefore, the system should generally be designed so that a user's error will not have serious consequences. The negative effects of errors should be controlled and minimized. The system should offer simple, comprehensible notification of the error, and simple, effective methods for recovery.

GLOSSARY

Adjustment controls: Controls used by maintenance personnel to correct or adjust the operation of equipment, such as to set an operating value. These controls may be external, such as controls mounted on maintenance panels, or internal, such as test and relay switches located on printed circuit boards.

Automatic mode: A mode in which processing proceeds without human intervention (as contrasted with a manual mode).

Automatic test equipment: Test equipment that checks two or more signals in sequence without the intervention of a maintainer. The test usually stops when the first out-of-tolerance signal is detected.

Bench mockup: An actual unit of equipment or replica used in training for checking or locating faults.

Built-in test: An integral part of a unit of equipment that performs diagnostic tests. Built-in test features may be as simple as a voltmeter, or as complex as an automatic checker.

Built-in test panel: A panel containing connections for external test devices so that internal components can be assessed.

Button: A type of hardware control device or a defined control region on the display screen which, when selected, causes some action.

Cannot duplicate: A classification given to a diagnostic test result when subsequent testing cannot produce the same result obtained in an earlier test.

Circuit breakers: Devices that protect equipment from excessive electrical current.

Circuit packaging: A method for organizing equipment into modules in which all parts of a single circuit or logically related group of parts, and only that circuit or group, are placed in a separate module.

Coding: Use of a system of symbols, shapes, colors or other variable sensory stimuli to represent specific information. Coding may be used (a) for highlighting (i.e., to attract a user's attention to part of a display), (b) as a perceptual indicator of a data group, or (c) to symbolize a state or attribute of an object (e.g., to show a temperature level or for warnings).

Collating test equipment: Test equipment that presents the combined results of two or more checks. For example, a light might come on only if a number of different signals are all within tolerance.

Component: A subdivision of a unit of equipment that can be treated as an object by the maintainer, but which can be further broken down into parts. A mounting board together with its mounted parts is an example of a component.

Component packaging: A method for organizing equipment into modules in which similar parts or components are located together; for example, all the fuses or all the relays might be grouped together.

Consistent fault set: The set of possible failures consistent with the given symptoms.

Continuous on-line self-test: A testing capability that continuously monitors overall system availability by rapidly identifying hardware failures.

Control: A mechanism used to regulate or guide the operation of a component, equipment, subsystem, or system.

Corrective maintenance: Maintenance tasks performed in response to a malfunction or the indication of a failure.

Display: A specific integrated, organized set of information. A display can be an integration of several display formats (e.g., a system mimic which includes barcharts, trend graphs, and data fields).

Display device: The hardware used to provide the display to users. Examples include video display units and speakers for system messages.

Enter: An explicit user action that affects computer processing of user entries. For example, after typing a series of numbers, a user might press an ENTER key that will add them to a database, subject to data validation.

Equipment packaging: The way that modules, components, and parts are arranged within an enclosure.

Fault-tolerant digital control systems: Digital systems with redundant processors that use fault-diagnostic routines that can detect single faults and isolate the failed equipment. This ensures that the equipment that is still operational takes over the control function.

Feedback: System or component response (e.g., visual or aural) which indicates the extent to which the user's desired effect was accomplished. Feedback can be either intrinsic or extrinsic. Intrinsic feedback is that which the individual senses directly from operating the control devices (e.g., clicks, resistance, control displacement). Extrinsic feedback is that which is sensed from an external source that indicates the consequences of the control action (e.g., indicator lights, display changes, aural tones).

Firmware: Computer programs and data loaded in a class of memory that cannot be modified by the computer during processing.

Functionally interchangeable units: Units of equipment that can perform the same function.

Fuses: Devices that protect equipment from changes in electrical current.

Go/no-go test equipment: Test equipment that provides one of two alternative answers to any question. For example, it may give a qualitative assessment of the condition of equipment by indicating whether a given signal is in (go) or out (no-go) of tolerance.

Hazardous condition: The presence of energy or a substance which is likely to cause death or injury by physical force, shock, radiation, explosion, flames, poison, corrosion, oxidation, irritation, or other debilitation.

Hazardous location: A space within a facility, room, or open environment where a hazardous condition exists.

Human factors engineering (HFE): The application of knowledge about human capabilities and limitations to the design of a plant, system, and equipment. HFE ensures that such designs, human tasks, and work environments are compatible with the sensory, perceptual, cognitive, and physical attributes of the personnel who operate, maintain, and support them (see human factors).

Human factors: A body of scientific facts about human characteristics. The term covers all physiological, psychological, and psycho-social considerations; it includes, but is not limited to, principles and applications in the areas of human factors engineering, personnel selection, training, job-performance aids, and human performance evaluation (see human factors engineering).

Human-system interface (HSI): The means through which personnel interact with the plant, including the alarms, displays, controls, and job-performance aids. Generically, this also includes maintenance, test, and inspection interfaces.

Hybrid human-system interface: A human-system interface that contains a combination of more traditional (e.g., analog and spatially dedicated) technologies and newer (e.g., digital computer-based) technologies.

Input: Information entered into a system for processing; the process of entering information; pertaining to the devices used to enter information.

Instrument cabinets and racks: Enclosures that hold modules, components, and parts. They typically have access doors or removable panels for access to their contents.

Labeling and marking: The use of labels and demarcations to identify units of equipment, modules, components, and parts.

Layout: The physical arrangement of the parts and components that make up a module or a unit of equipment.

Line-replaceable unit: An aviation term used to describe the smallest unit of equipment that can be replaced by personnel at an aircraft. A line-replaceable unit may consist of a box with mechanical and electrical connections.

Logical flow packaging: A method for organizing equipment into modules in which circuits, parts, and components are packaged and arranged in correspondence with their functional relationships.

Maintainability: The design of equipment to support effective, efficient maintenance activities.

Maintenance: A process with the objective of preserving the reliability and safety of NPP structures, systems, and components or restoring that reliability when it is degraded.

Manual mode: A processing mode in which the user is assumed to provide all inputs (as contrasted with an automatic mode).

Microprocessor: A small computer processor composed of integrated circuit technology.

Mistake: An error in intention formation, such as forming one that is not appropriate to the situation. Mistakes are related to incorrectly assessing the situation or inadequately planning a response.

Mode error: Performing an operation that is appropriate for one mode when the device is in another mode. Mode errors occur when the user believes the device is in one mode when it is actually in another and, as a result, performs an input action that is inappropriate for the actual mode.

Modularization: The separation of equipment into physically and functionally distinct units that can be easily removed and replaced.

Module: An assemblage of two or more interconnected parts or components that comprise a single physical entity, such as a printed circuit board, with a specific, singular function.

Mounting: The positioning and attachment of parts, components, and modules.

On-line maintenance: Maintenance performed while the plant is at power.

Output: The data which are the product of an information-handling operation or series of operations; the data emitted from a storage device; the data being transferred from primary storage (core, drum) to secondary storage (cards, tape); electrical pulses; reports produced by a printer or typewriter unit; a general term for output media, such as cards and tape. Contrasts with Input.

Packaging: The grouping of functions, components, and parts into units or modules.

Part: An object that cannot normally be broken down further without destroying its designated use. Fuses, transistors, resistors, and capacitors are examples.

Physically interchangeable units: Units of equipment that can fit into the same mounting position or fixture.

Preventive maintenance: Scheduled tasks, such as inspection, service, adjustment, calibration, and replacement, intended to keep equipment in condition for operational or emergency use. Contrasts with corrective maintenance.

Printed circuit board: A module organization in which parts are mounted on an integrated circuit board.

Programmable logic controller: A digital controller that uses a microprocessor to process signals.

Schema: A sequence of linked behaviors that, through repeated performance or deliberate training, becomes somewhat automatic to the individual. A schema may be executed when the type and strength of the stimulus matches the trigger conditions of the schema.

Service points: Equipment locations used for performing routine maintenance tasks, such as adjusting, cleaning, or replacing components.

Software errors: Instructions that exist in computer code that can cause undesirable behavior of a computer-based system.

Shock mounts: Energy-absorbing attachment devices that reduce vibration of the attached equipment.

Should and may: The word "should" is used to denote a recommendation; the word "may" is used to denote permission; it applies to a characteristic that is acceptable but not necessarily recommended (e.g., a preferable alternative may exist).

Simulation-oriented, computer-based instruction: A training technique that presents a two-dimensional, interactive depiction of the particular equipment trainees are learning to troubleshoot.

Slip: An error in carrying out an intention. Slips result from "automatic" human behavior, when schema, in the form of subconscious actions that are intended to accomplish the intention, get waylaid en route. Thus, while one action is intended, another is accomplished. The highly practiced behavior of an expert leads to the lack of focused attention that increases the likelihood of some forms of slips.

Soft control: A control device that has connections with the control or display system mediated by software rather than direct physical connections. As a result, the functions of a soft control may be variable and context-dependent rather than statically defined. Also, the location of a soft control may be virtual (e.g., within the display system structure) rather than spatially dedicated. Soft controls include devices activated from display devices (e.g., buttons and sliders on touch screens), multi-function control devices (e.g., knobs, buttons, keyboard keys, and switches that perform different functions depending upon the current condition of the plant, the control system, or the HSI), and devices activated via voice input.

Split-half test: Theoretically the most efficient test that a fault-finder can perform because it eliminates one-half of the items from the consistent fault set.

Subsystem: A collection of modules that perform a particular function.

System: An integrated collection of plant components and control elements that operate together and possibly in conjunction with other systems to perform a function.

System response time: The elapsed time between the initiation of a command and the notification to the user that the command has been completed.

Test equipment: Diagnostic tools used to assess the status of equipment and locate faults that may be present.

Test points: Equipment locations used for conducting tests to determine the operational status of equipment and for isolating malfunctions. Test equipment may be connected at these points.

Text: The primary display for word processing, consists of alphanumeric character strings in linear arrays, making up words, sentences, and paragraphs. The main body of printed or written matter on a page or in a message.

Unit of equipment: An assemblage of items that may include modules, components, and parts that are packaged together into a single hardware package.

Value: Specified data for a particular parameter or variable.

Variable: A quantity that can assume any of the given set of values.

Watchdog timer: An electronic self-testing feature that detects when an expected electrical signal is not received within an expected period, thus indicating a possible malfunction.

Workload: The physical and cognitive demands placed on plant personnel.

Workstation: The physical console at which a user works.